THE MEDICAL INFORMATION PROTECTION AND RESEARCH ENHANCEMENT ACT OF 1999

HEARING

BEFORE THE

SUBCOMMITTEE ON
HEALTH AND ENVIRONMENT

OF THE

COMMITTEE ON COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

JULY 15, 1999

Serial No. 106–53

Printed for the use of the Committee on Commerce

U.S. GOVERNMENT PRINTING OFFICE
58–501CC WASHINGTON : 1999

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-059576-2

COMMITTEE ON COMMERCE

TOM BLILEY, Virginia, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana
MICHAEL G. OXLEY, Ohio
MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
Vice Chairman
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
BRIAN P. BILBRAY, California
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
TOM A. COBURN, Oklahoma
RICK LAZIO, New York
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING,
Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
RON KLINK, Pennsylvania
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
THOMAS C. SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN McCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DeGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California

JAMES E. DERDERIAN, *Chief of Staff*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON HEALTH AND ENVIRONMENT

MICHAEL BILIRAKIS, Florida, *Chairman*

FRED UPTON, Michigan
CLIFF STEARNS, Florida
JAMES C. GREENWOOD, Pennsylvania
NATHAN DEAL, Georgia
RICHARD BURR, North Carolina
BRIAN P. BILBRAY, California
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
TOM A. COBURN, Oklahoma
Vice Chairman
RICK LAZIO, New York
BARBARA CUBIN, Wyoming
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING,
Mississippi
ED BRYANT, Tennessee
TOM BLILEY, Virginia,
(Ex Officio)

SHERROD BROWN, Ohio
HENRY A. WAXMAN, California
FRANK PALLONE, Jr., New Jersey
PETER DEUTSCH, Florida
BART STUPAK, Michigan
GENE GREEN, Texas
TED STRICKLAND, Ohio
DIANA DeGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
LOIS CAPPS, California
RALPH M. HALL, Texas
EDOLPHUS TOWNS, New York
ANNA G. ESHOO, California
JOHN D. DINGELL, Michigan,
(Ex Officio)

Public laws | Hearings | House | 106th Congress | 1st session | 1999

CMS Library
C2-07-13
7500 Security Blvd.
Baltimore, Maryland 21244

CONTENTS

Page

Testimony of:
- Andrews, Elizabeth B., Director of Worldwide Epidemiology, Glaxo Wellcome Inc 138
- Appelbaum, Paul, Professor and Chair, Department of Psychiatry, University of Massachusetts Medical School, on behalf of the American Psychiatric Association 32
- Carty, Cristin, Vice President, California Health Institute 127
- Feldblum, Chai, Professor of Law and Director, Federal Legislation Clinic, Georgetown University Law Center 38
- Frey, Carolin M., Chairman, Institutional Research Review Board, Pennsylvania State Geisinger Health System 148
- Johnson, Randel K., Vice President, Labor and Employee Benefits, U.S. Chamber of Commerce 131
- Koski, Greg, Director, Human Research Affairs, Partner Health Care System, Massachusetts General Hospital 143
- Nielsen, John T., Senior Counsel and Director of Government Relations, Intermountain Health Care 19
- Pawlak, Linda, parent 31
- Tang, Paul C., Medical Director, Clinical Informatics, Palo Alto Medical Clinic 27

Material submitted for the record by:
- Shays, Hon. Christopher, a Representative in Congress from the State of Connecticut, prepared statement of 164

THE MEDICAL INFORMATION PROTECTION AND RESEARCH ENHANCEMENT ACT OF 1999

THURSDAY, JULY 15, 1999

HOUSE OF REPRESENTATIVES,
COMMITTEE ON COMMERCE,
SUBCOMMITTEE ON HEALTH AND ENVIRONMENT,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2322, Rayburn House Office Building, Hon. Michael Bilirakis (chairman) presiding.

Members present: Representatives Bilirakis, Upton, Greenwood, Burr, Bilbray, Ganske, Norwood, Coburn, Cubin, Bryant, Brown, Waxman, Stupak, Green, DeGette, Barrett, Capps, Hall, and Eshoo.

Also present: Representative Markey.

Staff present: John Manthei, majority counsel; Marc Wheat, majority counsel; Cliff Riccio, legislative clerk; and John Ford, minority counsel.

Mr. BILIRAKIS. The hearing will come to order. Good morning.

I would like to first thank all of our witnesses for joining us today, and particularly Justin Pawlak and his mother Linda. The purpose of this hearing is to explore the issues of medical confidentiality.

Today we will have an opportunity to examine H.R. 2470, which is the Medical Information Protection and Research Enhancement Act of 1999.

I would like to start by commending our colleague Jim Greenwood for drafting this legislation and also to recognize the efforts of Congressmen Upton, Shays, Norwood and Burr in working with him to address this very complicated issue.

As you know, the Health Insurance Portability and Accountability Act of 1996 set a deadline for Congress to pass legislation addressing the confidentiality of individual identifiable health information. Unless Congress acts by August 21, the Secretary of Health and Human Services is directed to issue regulations within 6 months to address the confidentiality of administrative data stored or transmitted electronically. Significantly, the Secretary's regulatory authority is limited to establishing standards for information that is transmitted and stored electronically, a more narrow focus than the comprehensive approach taken in the bill before us.

While the modern health care delivery system is increasingly electronic, as we well know, most patient health information remains paper based. We all know that medical records contain very personal and sensitive information. Certainly this information

must be safeguarded and any abuse of it cannot be tolerated. However, we must also ensure that increased protections do not inadvertently jeopardize the quality of health care in this country. Any legislation must take into account the highly integrated and complex nature of our health care system.

In our previous hearing, I emphasized the need to develop responsible legislation to safeguard confidential medical information and to impose tough penalties for abuse. We must ensure strict accountability for the use of this information while preserving the ability to conduct important medical research.

I believe that H.R. 2470 is a significant step forward in accomplishing these goals and I hope that it serves as a starting point for legislative action on a truly bipartisan basis.

Again, I would like to thank all of our witnesses for taking time to be here. I would now recognize the ranking member, Mr. Brown from Ohio.

Mr. BROWN. Thank you, Mr. Chairman, for holding this hearing and I would like to thank the witnesses also for joining us today.

I am glad that we are taking up the issue of medical records privacy. The statutory deadline is about 5 weeks away, which means we have no time to spare. I am disappointed the majority chose to focus on only one of the privacy bills. It is my experience that it is unusual to limit a legislative hearing to one bill when other initiatives have also been introduced: H.R. 1941, the bill sponsored by Mr. Condit of California, which had 57 cosponsors, and Mr. Markey of Massachusetts has a bill, H.R. 1057, that has 41.

These are other privacy bills that deserve the same consideration that we are giving to H.R. 2470. The best way to make progress is to compare H.R. 2470 to the bill of Mr. Condit. The key difference between those two bills are the core issues in the privacy debate:

Should individuals have a private right of action when their medical records have been exploited? H.R. 2470 does not establish this right. Mr. Condit's bill does. Rights that can be denied without remedy are not rights, they are only hopes.

Should privately funded research be treated differently from publicly funded research when it comes to protecting the confidentiality of medical information? H.R. 2470 says yes; Mr. Condit's bill says no.

What would a participant in privately funded research say? I am guessing that participant would assume and expect the same level of protection regardless of who funds the research. The goal is not to establish basic privacy protections for some individuals, it is to establish them for all individuals.

Should Federal privacy laws preempt stronger State laws? H.R. 2470 says yes; our bill says no.

States are typically the first to identify consumer issues, and they are the innovators when it comes to addressing them. Federal protection should function as the floor, not the ceiling, for medical privacy protections.

I look forward to hearing our witnesses with respect to these issues and what I hope will be a productive and balanced hearing.

Mr. BILIRAKIS. Mr. Greenwood for an opening statement.

Mr. GREENWOOD. Thank you, Mr. Chairman. The title of the legislation that we are considering today is the Medical Information Protection and Research Enhancement Act and it is important to understand that those two goals are what we mean to accomplish here. Obviously the personal security and the well-being of every American will be profoundly improved if we succeed in accomplishing these dual purposes.

First on the privacy issue, our medical records contain personal, sensitive, potentially humiliating information, which if misused could cause discrimination in the workplace and adversely affect one's ability to purchase insurance. For that reason we create in this legislation the definition of the term "protected health care information" to make sure that it is kept private and to make sure that there are remedies and penalties for its misuse.

Second, the second goal, every one of us and every American in America, every one of our family members, will benefit from, continue to benefit from the ability of researchers, assurers of quality and others to use the awesome power of information processing to study health outcomes and thereby discover new and better treatment modalities and ways to deliver health care as effectively and efficiently as possible.

With the wrong public policy, these two admirable and critical goals are competing adversaries. With the right public policy, they are complementary colleagues. As has been mentioned, we do confront on August 21 a deadline, the 1996 Kennedy-Kassebaum Health Insurance Portability and Accountability Act sets that date, and if we do not accomplish a legislative remedy, the Department will issue regulations. Of course, that will be insufficient because it only applies to electronic records, and most medical records are not electronic but in fact still on paper.

The policy incorporated in H.R. 2470 does the following: It establishes the individual's right, which does not currently exist at the Federal level, to inspect, copy and amend his or her patient records. That is brand new. It enacts strong uniform Federal standards which replace conflicting State laws and impose strong civil and criminal penalties for the misuse of these records, the remedies to which Mr. Brown refers; requires law enforcement officials to demonstrate legitimate need in order to obtain protected health information; and protects patients involved in medical research trials when ensuring information can be used to continue research breakthroughs.

The question has been raised and will be raised throughout this hearing: Why State preemption? Why is it important for the Federal Government and Congress to establish a unified standard: The founders of our Constitution recognized the need to protect interstate commerce.

The logic of the commerce clause is plain sense. It made sense to ensure that buggy whips and butter churns could be transported across State lines without being subjected to the micro management of 13 colonies. It certainly is plain that medical data transmitted at the speed of light across 50 States and the District of Columbia requires a uniform standard that ensures both privacy and utility. I believe every member of this committee shares the twin goals of protecting privacy and enhancing research.

H.R. 2470 is not the first bill drafted toward these ends and it will not be the last, but I have every confidence that if we reach across the aisle toward one another in good faith and with a positive, constructive approach, we can produce a final product that is worthy of us all, and I pledge to work with all of my colleagues on both sides of this committee toward that end.

Two footnotes: I would like to draw attention to a drafting oversight in the last draft the inadvertent elimination of workplace information protections, and I would like, Mr. Chairman, to submit a letter indicating my desire to correct that in the next draft.

Mr. BILIRAKIS. Without objection, so ordered.

[The information referred to follows:]

CONGRESS OF THE UNITED STATES
HOUSE OF REPRESENTATIVES
July 14, 1999

DEBORAH V. DIBENEDETTO, MBA, RN, COHN-S, ABDA
President
American Association of Occupational Health Nurses, Inc.
2920 Brandywine Road
Atlanta, Georgia 30341-4146

DEAR MS. DIBENEDETTO: When drafting H.R. 2470, the Medical Information Protection and Research Enhancement Act, an oversight was made that excluded protections for medical information used in the workplace. Clearly this type of information is extremely sensitive and can be used to discriminate not only against employees, but for occupational health nurses and other providers who sometimes must weigh the threat of losing their job against protecting the information of their coworkers.

As originally drafted, the bill ensured that the disclosure of the protected employee health information within the entity is compatible with the purpose for which the information was obtained and limited to information necessary to accomplish the purpose of the disclosure. In addition, the draft legislation also required the employer to prohibit the release, transfer or communication of the protected health information to officers, employees, or agents responsible for hiring, promotion, and making work assignment decisions with respect to the subject of the information. It was unfortunate these protections were inadvertently removed in the final version of the bill. It is my intention to do all in my ability to add these protections back in to H.R. 2470.

I look forward to working with you in the future on this critical patient protection. Please do not hesitate to contact me should you have additional questions or concerns.

Sincerely,

JAMES C. GREENWOOD

Mr. GREENWOOD. And I would like to take the opportunity to introduce to our panel Justin Pawlak. He is the young man in the center of the table there. I have learned that Justin wants to run for Congress someday. And, Justin, I will let you know when it is your turn.

Thank you, Mr. Chairman.

Mr. BILIRAKIS. Thank you. Mr. Waxman for an opening statement?

Mr. WAXMAN. I will yield to Ms. Eshoo.

Ms. ESHOO. Thank you, Mr. Waxman, and thank you, Mr. Chairman, for holding this important hearing today.

As I was walking into the Rayburn building this morning, I thought that the last several hearings and/or markups that I have been to have dealt with the issue of privacy, and here we are again on the issue of privacy as it relates to medical records.

I would like to begin by recognizing my constituent, Dr. Paul Tang of Palo Alto, California. Welcome. It is a pleasure to see you

here. I also want to welcome Cristin Carty who does superb work with the California Health Care Institute. They have taken their place in a prominent way in working with members and providing a great deal of the research and information that members need in order to make informed decisions.

With the advent of managed care increasing, numbers of people are involved in health care treatment, payment and oversight, giving them direct access to often very sensitive medical information.

Today we have to place our trust in entire networks of insurers and health care providers. And I don't think that we can any longer expect that information supplied to our doctors will indeed remain confidential. The American people expect, and I think they are entitled to confidential, fair and respectful treatment of their private health information. It is incumbent upon Congress to enact a strong uniform Federal standard of protection for medical records privacy.

Currently, of course, there is no Federal standard, and the existing patchwork of State laws provide erratic protection at best.

Unfortunately, I don't think that my colleague Mr. Greenwood's bill is the total answer. Rather than providing privacy protections for medical records, the bill in fact, I think, steps back from the issue of medical privacy. The bill would allow insurers to use our private health information without consent for anything that can be called, "health care operations." It is a very, very broad term that is not defined in the bill. The bill is written in such broad terms that virtually anything the health plan writes into its contracts could be considered a health care operation.

For example, a health plan could include a contract clause that says health information will be used for marketing purposes. Or information can be used for insurance underwriting, allowing one to be rated as a bad risk and harming their ability to get insurance in the future. It is a very, very sensitive area for the American people.

Another major problem, as I see it, with the bill is the lack of enforcement. Providing for a right of action would give every American the basic right to seek redress for violations of their private medical records and yet the bill is silent. It is often said that silence is deafening. The bill is silent on this issue.

I would ask what good is a right if it can't be enforced? I think we should all think about that instead of scurrying to ideological corners. Just apply it to oneself. What good is it to have a right unless there is an ability to enforce it?

I too want to ensure that research is not hampered. I see firsthand, day in and day out in my very distinguished congressional district, the enormous good and the impact of that good the research does day in and day out. But I think we need to be sure that any legislation enacted doesn't erect any unnecessary barriers that would slow and impede medical research, and I think we can do both. I don't think that we have to do one at the cost of the other. But I don't think that we can risk the privacy of every American to keep their most personal medical records private.

Again, I think we need to establish a strong Federal standard to protect against unauthorized uses of our private health information

while remaining mindful of the effect our laws will have on medical research and the lives it can and does save every day.

Thank you, Mr. Chairman, for your leadership in this subcommittee. I think we have a ways to go in terms of hammering out something if in fact we are going to do that before the laws on the book would allow the Secretary to do so.

I look forward to working with you and other members of our committee to produce something not only for the full committee, but the full Congress that we can really be proud of. Thank you very much.

Mr. BILIRAKIS. I thank the gentlelady. And we will, if we are willing to work together.

Mr. Upton for an opening statement.

Mr. UPTON. I have a statement for the record. I would just like to add that I have very strong support for this, and allowing Jim Greenwood to lead this charge in a bipartisan way was terrific. He has been a good leader.

[The prepared statement of Hon. Fred Upton follows:]

PREPARED STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. Chairman, thank you for holding today's hearing on the Medical Information Protection and Research Enhancement Act. I also want to commend our colleague, Jim Greenwood, has shown in developing the comprehensive, thoughtful bill we will be discussing this morning. I am pleased to be a cosponsor of this legislation.

I am sure that developing this legislation was no easy undertaking. It must reflect a delicate balance between the need to ensure the privacy of individuals' medical information and the need that arises to use personally identifiable health information in biomedical research, to evaluate the safety and effectiveness of treatments and coordinate the delivery of health care, and for other legitimate purposes.

I am looking to hearing from our witnesses today about their perspective on achieving this balance.

Mr. BILIRAKIS. Mr. Waxman.

Mr. WAXMAN. Thank you. I am pleased that we are meeting today to discuss medical records legislation. Ensuring medical privacy in our multifaceted health care system is a vital patient protection. That is why I join together with Representative Gary Condit, Ed Markey, John Dingell, Sherrod Brown and others who have introduced consensus legislation that addresses the complex issues related to medical privacy in a commonsense manner.

Strong Federal privacy protections for medical records are critical to ensuring that our health care system operates effectively. Currently, only a patchwork of State laws address medical privacy matters and many of these provide minimal protections. As a result, individuals are withholding information from their health care providers, even avoiding care for fear of privacy violations.

Unfortunately, the majority's proposal, H.R. 2470, would only exacerbate individual's concerns. Among other provisions, H.R. 2470 would allow health insurers to use an individual's information for insurance underwriting and marketing without an individual's consent, and for health research without an individual's consent or any review of the research. It would override carefully crafted State laws which protect the privacy of sensitive information such as dental health records, genetic information and HIV test results and it would block States' ability to address such issues in the future.

I think it is important to have increased uniformity by enacting a strong Federal standard, but it is ironic to hear the Republicans deny the State's ability to act beyond that. Congress, I think, acted on this issue over 30 years ago. We may not act on it again for another 30 years. In the meantime the States ought to be able to respond to matters that come up that are unforeseen. Who would have thought about the AIDS epidemic even 15 or 20 years ago?

I believe the Congress can and should enact legislation that provides the appropriate balance between ensuring privacy protections for individuals' health records, allowing appropriate access to health information for public interest purposes, and ensuring that the States have the flexibility to address specific privacy concerns.

The Condit-Waxman-Markey-Dingell-Brown bill achieves this balance. Unfortunately, H.R. 2470 does not. I hope Congress moves forward on meaningful medical privacy legislation. As many here today know, the Health Insurance Portability and Accountability Act of 1996, known as HIPAA, set an August 21, 1999 deadline for passage of such legislation. It is unclear whether we are going to meet that deadline because none of the relevant committees in the House or Senate have reported out legislation.

Under HIPAA, if Congress fails to meet this deadline, the Secretary of HHS must promulgate regulations to protect medical privacy. The Secretary has issued recommendations that likely would be the basis of such regulations. These recommendations provide for strong privacy protections in many areas. Given the pressing need for Federal privacy protections, the Secretary should move forward with these regulations if Congress does not meet its deadline.

The worst case scenario would be for Congress to enact weak medical privacy legislation or for Congress to both push the deadline back for passage of legislation and prevent the Secretary from moving forward. This would leave millions of individuals with minimal assurances of medical privacy protections. There is no good policy reason for taking either approach.

I will continue to press forward with H.R. 1941 and I look forward to discussing this and other bills with today's witnesses. And of course, Mr. Chairman, even though this hearing is unfortunately being held only on the Republican bill, I hope this subcommittee will work in a bipartisan fashion, if that is possible, to try to work out a consensus. I never thought that medical privacy was a partisan issue. It should not be. It is a matter that we should be working on together to find a place where we can accomplish the goals that I think all of us share. Thank you very much.

Mr. BILIRAKIS. I thank the gentleman. Mr. Norwood.

Mr. NORWOOD. Thank you very much and thank you for having this hearing. I would like to thank Congressman Greenwood for his hard work. For the panelists who have come a long way, we are grateful. We appreciate your help today.

But, Justin, we especially need your help. Anything you can do will be greatly appreciated by us all. Protection of private medical information obviously is a very important issue, and I believe this bill will bring us significantly closer to resolving the issue before the statutory deadline. We all know that if we do not meet our August deadline, the Secretary of HHS will take the job out of our

hands and impose regulations that we have no control over. We are all aware of the potential dangers of allowing this to occur. The administration says that it wants to protect patients' rights to privacy. However, the administration has also considered a proposal to assign to each citizen a unique health identification number to track each person's medical information electronically. We should be very mindful of the consequences of Congress defaulting this responsibility to the Secretary.

One of the issues that I believe the Greenwood bill deals with well is that of State law. If someone lives and works in Washington, DC, goes to the doctor in Arlington, picks up their prescription in Bethesda, what are the consequences of having three different sets of rules governing that one doctor's visit? Considering the interstate nature of medical records and the fact that 50 percent of Americans live on the border of their State, this issue should be considered within the context of interstate commerce.

This is why I strongly support the preemption clause in the bill. That is why I am a strong believer in allowing State laws to govern the practice of medicine. I believe that a uniform standard is one more appropriate to govern the movement of medical information. Opponents of this bill are going to have problems with the fact that private cause of action for misuse of records has been left out of the bill. They may try to use this as an excuse to stall the bill. I am not saying whether I would vote for or against an amendment to include a Federal cause of action, but I do know that we have here the perfect chance for us to discuss the way we deal with penalties.

We must also keep in mind that the bill does have a provision allowing criminal prosecution. I wondered and have wondered sometimes if that might not have been a better route for managed care reform. Frankly, Mr. Chairman, the complexities of this issue, especially compounded with our time restraint, make managed care reform look like child's play. I feel that this bill is a viable solution to this issue and should be given everyone's serious and open-minded consideration.

I look forward to working with you, Mr. Chairman, and Mr. Greenwood and hope that we will get this done and save the Secretary a lot of effort. Thank you very much.

[The prepared statement of Hon. Charlie Norwood follows:]

PREPARED STATEMENT OF HON. CHARLIE NORWOOD, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

I'd like to begin by thanking the Chairman for holding this hearing. Protection of private medical information is an important issue, and I believe that this bill will bring us significantly closer to resolving the issue before the statutory deadline.

We all know that if we do not meet our August deadline, the Secretary of HHS will take the job out of our hands and impose regulations that we have no control over. We are all aware of the potential dangers of allowing this to occur. The administration says that it wants to protect patients' rights to privacy; however, the administration has also considered a proposal to assign each U.S. citizen a unique health identification number to tag and track each person's medical information electronically. We should be very mindful of the consequences of Congress defaulting this responsibility to the Secretary.

One of the issues that I believe the Greenwood bill deals with well is that of state law. If someone lives and works in Washington, DC, goes to a doctor in Arlington, and picks up a prescription in Bethesda, what are the consequences of having three different sets of rules governing that one doctor visit? Considering the interstate na-

ture of medical records, and the fact that fifty percent of Americans live on the border of their state, this issue should be considered within the context of interstate commerce. This is why I strongly support the preemption clause in the bill. While I am a strong believer in allowing state laws to govern the practice of medicine, I believe that a uniform standard is more appropriate to govern the movement of medical information.

Opponents of this bill are going to have problems with the fact that private cause of action for misuse of records has been left out of the bill. They may even try to use this as an excuse to stall the bill. I'm not saying whether I would vote for or against an amendment to include a federal cause of action, but I do know that what we have here is the perfect chance for us to discuss the way we deal with penalties. We must also keep in mind that the bill does have a provision allowing criminal prosecution. I wonder sometimes if that might not have been a better route for managed care reform.

Frankly, Mr. Chairman, the complexities of this issue, especially compounded with our time constraint, make managed care reform seem like child's play. I feel that this bill is a very viable solution to this issue and should be given everyone's serious and open minded consideration.

I look forward to the witnesses testimony and yield back the balance of my time.

Mr. BILIRAKIS. I thank the gentleman. Ms. Capps.

Ms. CAPPS. Good morning. I want to thank the chairman for holding this important hearing and welcome our distinguished witnesses here today.

I also want to mention Cristin Carty because I have worked closely with her. She has been very helpful on a variety of health-related issues.

Medical privacy is a difficult and complex issue. On the one hand it is so imperative that we prevent the misuse of patients' medical data. I believe strongly that we need to establish a national policy that safeguards an individual's right to privacy with respect to personally identifiable health information. The misuse of health information can harm patients and families. Unauthorized use of our health plans, genetic information or our family history, can make it difficult, if not impossible, for many Americans to obtain health insurance. Patients need to be encouraged, have the right to be encouraged to share with their doctors, nurses or therapists all of their health information. No diagnosis or treatment is complete without it. But if patients can't be sure that this sensitive and personal information will be kept confidential, they will not be forthcoming. That will hurt patient care. And it will stifle research efforts. Privacy must never take a back seat to profits.

I am supportive and mindful of the needs of the research community as well. The University of California at Santa Barbara, for example, is an academic center in my district, and I want very much to encourage their research efforts there and not to impede their work. I have a personal interest in this topic. I have a daughter who is involved in a clinical trial at Stanford, and her life may hang in the balance of that research.

The Medical Information Protection and Research Enhancement Act of 1999 was introduced just this week. It is a complex bill and I am still evaluating it, but I do have some initial concerns. It appears that the bill does not provide individuals the basic right to seek redress for privacy violations, as it does not provide for a private right of action. It also appears to contain inadequate provisions regarding an individual's right to notice of a health plan's confidentiality practices requiring that a health plan need only post

such a notice instead of ensuring that each individual receive a copy.

I look forward to discussing these issues at this hearing. As we navigate this complex medical privacy issue, I know we must be very careful to protect patients. We in Congress must make every effort to maintain the public trust, but we should also encourage research. This is often a difficult balance to strike. But I do believe that it is the duty of this subcommittee to reach that balance. I yield back the balance of my time.

Mr. BILIRAKIS. I thank the gentlelady. Mr. Bryant.

Mr. BRYANT. Thank you, Mr. Chairman. Before I yield back the balance of my time, I want to thank you for holding this hearing and Mr. Greenwood for his hard work on this bill and I want to thank the distinguished panelists here today. Thank you, Mr. Chairman.

Mr. BILIRAKIS. Thank you. Ms. DeGette.

Ms. DEGETTE. Thank you, Mr. Chairman. I am grateful that you held this hearing today on what has developed into a critical issue. I want to thank Mr. Greenwood also for introducing this legislation and for his hard work in getting this discussion started and also those on my side of the aisle for their many years of work on medical privacy.

I think that without strong medical privacy protections, the privacy of health care consumers and the integrity of medical research are at risk. Medical privacy, as has been so aptly noted by my colleagues, is an intricate matter and the devil is in the details.

Consumers should not have to worry that their private medical records will be exploited in marketing schemes or used to deny insurance applications if they have not signed the necessary documents. We have a good opportunity to make these protections more clear so consumers do not face discrimination or inappropriate invasions of their privacy, and so they are not left questioning what do I sign, who is looking at my file, what was I not told, and what should I be doing.

This is a very delicate balance, as we all know: strong consumer protections that reassure the public that its privacy will not be invaded, and also tempered regulated access to medical records so that researchers and law enforcement officials can do their jobs.

I am particularly concerned that any medical privacy legislation will establish provisions that ensure the integrity of medical research. While some have said that research needs and privacy concerns cannot be merged, I think that in actuality the two needs are really not that far apart. If we fail to reassure the public that medical records will be used prudently and that the privacy of individuals will be preserved, then the public will refuse to open the records to researcher. While there is much to consider in evaluating the implications medical privacy protections have on research, I am particularly troubled that some have criticized proposals that require an institutional review board or similar entity to review and approve research utilizing medical records. Such entities can ensure that the potential good of the research outweighs any privacy concerns and that strong privacy protections are in place by preserving the confidentiality of the data that is collected. IRBs and other like entities are used in almost every research setting.

In fact, many organizations that privately fund research insist on an IRB to safeguard the reliability of the research.

I think that it is naive to believe that requiring such a check would negatively affect anything other than the marketing plan for the researcher's resulting product. And I am puzzled that some are anxious to differentiate between privately and publicly funded research for IRBs and other privacy protection requirements. It seems to me that, if one were to have stronger privacy protections than the other, patients would be reluctant to participate in research that could inappropriately disclose private information. But once again, as has been noted in this hearing and by me, the devil is in the details, and I don't think that the burden should be placed on the American public to determine what the source of the funding is for the research and therefore what the implications for the funding source holds on their privacy of their records.

So, therefore, I look forward to hearing what our panelists have to say about medical privacy proposals on research needs, and how this is going to impact patients.

With that, Mr. Chairman, I yield back the balance of my time.

Mr. BILIRAKIS. Thank you. Dr. Ganske.

Mr. GANSKE. Thank you, Mr. Chairman. Well, if there is a tough problem to figure out what to do in the right way on Capitol Hill, the hardest one that I have seen since I have been in Congress is the issue of the right balance and walking the right line on medical privacy.

I looked at this issue a lot when I was drafting my patient protection legislation and decided it was such a complex issue that I could not include a substantive provision in that bill or I would have something that was 200 pages long.

And then, of course, we got into the debate on H.R. 10, and I see my good friend and colleague from Massachusetts waiting to say a few words, so I want to say a few words about the medical privacy issue on H.R. 10 because there is some reference to that in the testimony today.

It is very interesting, I am somewhat amused that there are those who think that the exceptions in order for an insurance company to do its business were too broad, and yet at the same time the chairman of the full committee is now getting letters from the insurance industry, saying if the exceptions are construed narrowly so as to exclude from the reach of the exception many aspects of the insurance business, the problems will be magnified since the opt-out provisions will apply to transfers integral to the business of insurance.

So on the one hand, those who are looking for a very comprehensive bill, which I thought was beyond the reach of what we are dealing with, a financial service entity, insurance, banking and securities, want to go—be much more strict in the exceptions, the insurance industry or at least some in the industry think that those exceptions were too strict. I don't know, Mr. Chairman. Maybe that is demonstrating that they were somewhere in the right range. I have, Mr. Chairman, a Dear Colleague that I would like unanimous consent to enter into the record and also to distribute to members of the committee.

Mr. BILIRAKIS. Without objection, so ordered.

[The information referred to follows:]

CONGRESS OF THE UNITED STATES
HOUSE OF REPRESENTATIVES
July 12, 1999

DEAR COLLEAGUE: The medical privacy provision in H.R. 10 restricts disclosures of customer health and medical information by insurers.

Some concerns have been raised about the exceptions to the opt-in policy. I would like to take this opportunity to define some of the terms found in the exceptions and dispel the misinformation that is being circulated regarding these provisions.

Under current law, an insurance company obtains medical record information only with an individual's authorization. The medical privacy provision in H.R. 10 relates to how an insurance company shares the data after it has acquired it. The provision states that insurers can only disclose this information with an individual's consent except for limited, legitimate business purposes. These provisions would apply to all insurers who are currently engaged in the insurance business, and who have millions of contracts in force right now. Without these exceptions, these insurers would no longer be able to serve their customers.

The exceptions include ordinary functions that insurance companies are already doing in their day-to-day business. Such operations include:

Underwriting: Insurers use health information to underwrite. The price someone pays for insurance is based in part on an individual's state of health. Insurers gather medical information about applicants during the application and underwriting process. Underwriting is fundamental to the business of insurance. During the underwriting process, an insurer may use third parties, such as labs and health care providers to gather health information and/or to analyze health information. The insurer may also use third parties to perform all or part of the underwriting process and must disclose information to these third parties, such as doctors or third party administrators, so that they can enter into the contract in the first place.

Reinsuring Policies: Insurance companies sometimes assume a "risk" and then further spread the risk by "reinsuring" a policy. While often a "reinsurance" arrangement is made at the initiation of a contract, there are also times when reinsurance occurs after the policy is issued. The reinsurer needs access to the first insurer's underwriting practices as part of its due diligence. Without this language, the wheels of the reinsurance industry could literally grind to a halt.

Account Administration, Processing Premium Payments, and Processing Insurance Claims: In order to pay a claim for benefits, the insurer has to process the claim. This is a basic business function. These activities are the very reasons an individual signs up for a policy in the first place. Companies may use third party billing agencies and administrators to process this information. A company that doesn't today, may tomorrow; and we need to ensure that they can, so that consumers can be served.

Reporting, Investigating or Preventing Fraud or Material Misrepresentation: There are certainly times when individuals may not want to disclose all of their health information for valid reasons. However, there are those that may try to hide health information relevant to whether a policy would be issued or what would be charged for that policy. For example, nonsmokers usually pay less for insurance than smokers. On the other hand, if you have a chronic illness your premium may be higher. If an individual is engaged in fraud of material misrepresentation, it is highly unlikely that they would give their consent so that the insurer could disclose this information, for example, to its law firm to undertake an investigation of the matter or to the insurance commissioner or other appropriate authorities.

Risk Control: Credit card companies and other financial institutions involved in billing, conduct internal audits to ensure the integrity of the billing system. During this process, the company verifies that merchants, credit card holders and transactions are legitimate. These audits are done on random samples in which transactions dealing with medical services are not segregated or treated differently from other types of transactions. However, if this exception were not included, the company would be prevented from verifying the validity of transactions dealing with medical services. This would open the door for much fraud and abuse or the inability for consumers to write checks or use credit cards to pay for medical co-payments.

Research: Insurers do research for many purposes. For example, life insurers will do research related to health status and mortality to help them more accurately underwrite and classify risk. This provision is needed so that insurers can continue to do research.

Information to the Customer's Physician: This exception is necessary to allow insurers to release information to an individual's physician. For example, during the

underwriting process, an insurer may conduct blood test on an applicant. If the blood tests indicate that there may be something wrong, the insurer needs to be able to share the information with the individual's designated physician or health care provider so that they, together, can determine the best course of treatment.

Enabling the Purchase, Transfer, Merger or Sale of Any Insurance Related Business: No one has a crystal ball. A company does not know in advance when they will engage in these activities. It would be impractical if not impossible to obtain the tens of thousands of authorization forms signed and returned to the company so that a company could purchase, transfer, merge or sell an insurance related business. Without this language, companies will not be able to serve their customers by forging new business frontiers. Since the privacy provision covers all insurance companies, the purchasing company will have to abide by the same restrictions as the original company.

Or as Otherwise Required or Specifically Permitted by Federal or State Law: There are some states that require or specifically permit the disclosure of medical information by insurance companies. For example, a company may have to disclose health information to a state insurance commissioner so that the commissioner can determine if the company is complying with state law banning unfair trade practices. A company may have information that would help the police in an investigation where they suspect an individual has murdered someone in order to collect life insurance benefits. This language is necessary for these and other important public interests.

I hope that this brief explanation of the exceptions to the strong "opt-in" provisions of the medical privacy provisions of H.R. 10 clears up some misperceptions. During floor debate, I said I would work to include explicit language stating that this provision does not prohibit the secretary of HHS from issuing regulations on medical privacy as specified by HIPAA.

Furthermore, I hope consensus can be achieved on a comprehensive medical privacy bill. However, I remain convinced that as new financial services entities that combine banking, securities and insurance are created by H.R. 10, it is important that personal health data can be shared inside, or outside, the company *only* with the patient's permission. That is what the Ganske Amendment did.

If you need additional information, please contact Heather Ellers at 5-4426.

Sincerely,

GREG GANSKE
Member of Congress

Mr. GANSKE. And this describes some of the specifics of the exceptions in H.R. 10 and what exactly they mean.

Mr. Chairman, I want to deal specifically with some of the testimony today as it relates to my amendment in H.R. 10. There is a statement that says law enforcement entities would enjoy virtually unfettered access to medical records and insurance companies could review individual records in performing marketing studies. The Ganske amendment in H.R. 10 allows insurance commissioners to enforce the privacy provisions. I don't think that they are going to allow law enforcement entities unfettered access to medical records. And in regard to the marketing studies, nowhere in the amendment in H.R. 10 is marketing even mentioned.

Then there is a statement, Why should life insurers be able to routinely access patients' entire medical records without patient consent or knowledge?

I would point out that my provision in H.R. 10 is an across-the-board opt-in so that within that financial services or outside of the financial services, in order for that insurance company to share that information, they have to get an okay from the patient. And I would also point out when a life insurer processes an application for life insurance, many health-related factors are taken into consideration in order to determine the risk evaluation of the individual in order to determine what the appropriate premium should be. That is what insurance underwriting is.

Then there is a statement, "No limitations on subsequent disclosures of medical records to nonaffiliated entities." I would point out that we were dealing with H.R. 10 which was dealing specifically with these financial entities. If we had tried to extend that to nonaffiliated entities, it would have been ruled nongermane for H.R. 10.

Then there is a statement, "nor does the legislation encourage the use of de-identified medical records" the reason that wasn't in my amendment is that insurance companies have been able to use that information to track specific individuals for underwriting purposes. And I think that is an issue that is appropriate for this debate.

Mr. BILIRAKIS. If I may interrupt the gentleman, we have a vote on the floor and we have at least another opening statement, and I would like to get through opening statements before we break.

Mr. GANSKE. Finally, the amendment will not insure that patients will receive notice of confidentiality and disclosure practices of the insurance companies. That claim is correct. The amendment does not include disclosure requirements because the provision included in title V of the bill requires a financial entity to disclose all privacy policies. That is where we fit that amendment in.

So I would hope that the members of this committee, as we deal with a larger comprehensive medical privacy bill will not reflexively think that we should not have something in that financial services bill related to it, something reasonable like I think my amendment was. Remember, I promised on the floor that I would in conference try to get in specific language that said nothing in H.R. 10 would preclude the Secretary from going ahead and issuing her regulations if Congress cannot come up with a comprehensive bill.

I yield back the balance of my time.

Mr. BILIRAKIS. I thank you. I would like to finish up the opening statements before we run over for a vote. I yield now to Mr. Markey who is not a member of the subcommittee, but who is very much involved in this issue.

Mr. MARKEY. Thank you, and I thank you for your continuing indulgence for allowing me to attend these sessions. I have a great interest in privacy issues as we see each profession intersect with the on-line revolution, and it is clear that we have to deal with it as a subject.

I would ask you to picture where your medical records are right at this moment. You probably would imagine a file that looks something like this, containing the documentation of your most personal and intimate details of your life: your health history. You probably imagine this file in your doctor's office or at your local hospital, locked away in a filing cabinet, the keys of it dangling around the neck of a trustworthy nurse who looks like your mother or your grandmother, the guardian of your medical records. That nurse looks like that first nurse you went to when you were 3. If this is the image you are picturing, let it go, for the reality of today's information age speaks of a very different tomorrow.

Today many medical records are no longer confined to the physical barricade of a steel filing cabinet. More and more, we are depending on technology to provide the security once provided by lock

and key and the motherly town nurse. As we approach the 21st century, we are moving toward an information-based economy where we are losing control of the ability to ensure that there is, in fact, a lock on who has access to the most personal information regarding our lives. So we need to be thoughtful in our approach to privacy. By being most attentive to the needs of commerce, we destroy the ability to control who we will be in the new millennium. What we are looking for is commerce with a conscience.

Last week we passed the financial modernization bill, H.R. 10, after a great deal of debate which centered around access to financial information and who ultimately controls where that personal information will go. While we made very limited progress in providing privacy protections to financial information, we took steps backwards in providing privacy protections to medical information.

Today we are conducting a legislative hearing on the medical confidentiality bill, H.R. 2470, introduced on Monday by Mr. Greenwood along with six cosponsors, and I am very pleased that we have a hearing on that subject. But I think it is also noteworthy that this committee has also produced another bill that Mr. Condit, Mr. Waxman and Mr. Dingell, and Mr. Towns, Mr. Brown and I and 57 other cosponsors have introduced on the very same subject. And I think it would be very helpful if that subject was also before the committee as well.

There is a good reason why consumer groups have cosponsored the bill that I just referred to. And that is that the bill that is under consideration today has the support of industry, but only industry. And there is a good reason. It requires no consent or even an acknowledgment from the patient of her privacy rights. Simply by seeking treatment or signing onto a health plan, you are unknowingly agreeing to disclose health information for an open-ended list termed health care——

Mr. BILIRAKIS. Mr. Markey, would you please summarize. You are entertaining us, but please summarize.

Mr. MARKEY. Well, the point that I would make in summary, Mr. Chairman, is that a wide-ranging debate would include a full discussion of other legislation which is also now before the Congress, although not before this panel at this time, and I would hope that we would be able to discharge that. And a horse is a horse of course, of course. And I thank you, Mr. Chairman, for allowing me to testify at this time.

[The prepared statement of Hon. Edward J. Markey follows:]

PREPARED STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MASSACHUSETTS

Mr. Chairman, thank you for calling this morning's hearing on The Medical Information Protection and Research Enhancement Act. I would also like to thank you and Mr. Brown for your continued indulgence in permitting me to sit in on these sessions, because, as you know, the issues of privacy protections in general, and medical records privacy in particular are very important to me.

If I were to ask you to picture where your medical records are right at *this* moment, you probably would imagine a file that looks somewhat like this containing the documentation of your health history which includes some of the most personal and intimate details of your life. You probably imagine this file in your doctor's office or your local hospital locked away in a filing cabinet, the keys to it dangling around the neck of a trustworthy nurse who looks like your mother or grandmother, the guardian of your medical records. If this is the image you are picturing—LET IT GO—for the reality of today's information age speaks to a very different tomor-

row. Today, many medical records are no longer confined to the physical barricade of a steel filing cabinet. More and more we are depending on technology to provide the security once provided by lock and key and the motherly town nurse.

As we approach the 21st century, we are moving toward an information based economy where we are losing the ability to control who has access to the most personal information regarding our lives. We need to be thoughtful in our approach to privacy. By being most attentive to the needs of commerce we destroy the ability to control who we will be in the new millenium. What we are looking for is commerce with a conscience. Last week we passed the Financial Modernization Bill, H.R. 10—a great deal of the debate centered around access to personal information and who ultimately controls where that personal information will go. While we made very limited progress in providing privacy protections to financial information, we took steps backward in providing privacy protections to medical information.

Today, we are holding a legislative hearing on the medical confidentiality bill H.R. 2470 introduced late Monday night by Mr. Greenwood along with 6 cosponsors—I am pleased to have the opportunity to debate the issue of medical privacy but I'm at a loss as to why we are only considering a Republican proposal with 6 cosponsors when two other bills—both introduced by members of this Committee—are not being considered. In March I introduced H.R. 1057 which has the support of 41 cosponsors and in May I joined Mr. Condit, Mr. Waxman, Mr. Dingell, Mr. Brown and Mr. Towns in introducing a consensus bill H.R. 1941 which is now up to 57 cosponsors. Both of these bills are endorsed by a variety of patient, provider and consumer groups while Mr. Greenwood's bill has the endorsement of industry and industry alone.

There is a good reason why those most concerned with patient privacy do not support the Greenwood bill. It requires no consent or even an acknowledgment from the patient of her privacy rights. Simply by seeking treatment or signing on to a health plan, you unknowingly agree to disclose personal health information for an open-ended list of items termed "health care operations". This bill provides no real privacy protections for subjects of private research projects and preempts stronger medical privacy protections in state law. Finally, this bill provides no private right of action for patients to seek damages for violations of breaches of confidentiality.

I am pleased to be here today to discuss this important issue but I'm disappointed that the other medical privacy bills sponsored by members of this Committee are languishing. It is my hope that the next legislative hearing on this issue will include the other bills offered by members of the Committee.

Thank you.

Mr. BILIRAKIS. Dr. Coburn.

Mr. COBURN. I want to make two points. Confidentiality of medical records is important; and when the American public does not have confidence that that confidentiality is there, people get hurt. And all I would explain to you is look at the HIV epidemic where we have half a million people in this country who have HIV, who should not have it, because we didn't instill the confidence that people's records were going to be held in confidence.

The second point I would make is that Jim Greenwood, in writing this bill, has the qualifications and the character to put patients and their information first.

And although Mr. Markey and others may disagree with some of the components of this bill, we could not ask another Member of Congress that has the qualifications for caring for people in his background to write such a bill. And you can have confidence that whatever bill comes out of this committee with Mr. Greenwood's signature on it will be one that does protect patients' confidentiality in a way that is fair, firm, and will protect their future.

And with I yield back the balance of my time.

Mr. BILIRAKIS. Thank you very much, Doctor.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. BARBARA CUBIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WYOMING

Mr. Chairman, I would like to thank you for calling this hearing. This is an extremely complicated, but vitally important issue that we must resolve ahead of the August 21 deadline imposed by HIPPA.

Americans cherish our privacy, particularly when our medical and personal histories are involved. Congress must move to pass sensible, but effective legislation, to protect paper and electronic medical records. In our move to ensure valid privacy concerns, legislation must also recognize legitimate research requirements. For any legislation to be effective, it must contain strong enforcement mechanisms.

Representative Greenwood's legislation strikes a balance between personal medical privacy and research needs. I appreciate the work that he has done on this issue, and the positive effects it will have for every American.

As we delve into this complicated issue today, I look forward to hearing the unique perspectives of our witnesses. Thank all of you for coming.

PREPARED STATEMENT OF HON. TOM BLILEY, CHAIRMAN, COMMITTEE ON COMMERCE

Thank you, Chairman Bilirakis for holding this hearing today on H.R. 2470, the Medical Information Protection and Research Enhancement Act of 1999. I commend my colleague on the Committee, Mr. Greenwood of Pennsylvania, for his foresight and diligence in bringing comprehensive legislation on this important issue to the Committee.

Mr. Greenwood has done an excellent job in improving language that has been crafted, reviewed, fought over, and agreed to over the last several years in the other body. This language has benefitted from a long discussion process among experts in the private and public sectors. It strives to preserve patient privacy, while assuring that medical research will continue to progress. This language is well understood by those in the advocacy community, and is the most well-mapped geography of all the medical record confidentiality legislation in Congress.

I wish that I could say the same for legislation that has been introduced by my colleagues on the other side of the aisle. Despite the best of intentions, the unintended consequences of bills like H.R. 1057 and H.R. 1941 could be very dire for patients across the country. According to written testimony submitted by the Biotechnology Industrial Organization at our last hearing on confidentiality, H.R. 1057, the Medical Information Privacy and Security Act, and H.R. 1941, the Health Information Privacy Act, "contain provisions that will significantly impede medical research by requiring that all research be monitored by an external entity." In fact, the testimony states, "H.R. 1941 would expand the Federal government's role in private research by requiring that all research, whether funded with private dollars or taxpayer dollars, be reviewed by an entity certified by the Secretary using standards that are *more restrictive* than that used by Institutional Review Boards."

We should not throw the baby out with the bathwater. In our efforts to ensure that medical records remain confidential, we should not make medical research so difficult and expensive that the cures patients seek are unavailable. I look forward to hearing from our witnesses today on how we can improve the Greenwood legislation to safeguard patient confidentiality while ensuring a vital medical research industry.

Thank you, Mr. Chairman, and I look forward to the testimony this morning.

PREPARED STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

I want to thank the Chairmen for scheduling this important hearing.

As the deadline imposed by HIPAA for Congressional action approaches, I believe it is important for this subcommittee to begin its consideration of specific legislative language.

Unfortunately, I believe the Republicans are making a mistake by essentially choosing to move a bill that does not have any bipartisan support and is filled with loopholes that could jeopardize our medical record privacy rights.

Mr. Chairman, Americans are scared of what will happen to them if their medical records fall into the wrong hands. And by the term "wrong hands", I am not talking about criminals—I am talking about potential employers and health insurance companies who discriminate against people based on their health history or even the likelihood of their future health status.

Today's information and technology gives the world an unprecedented opportunity for health research and prevention. Efforts like the human genome project has the potential to provide scientists and doctors with levels of health information that was inconceivable less than ten years ago.

However the benefits of the genome project and other research efforts will be limited if Americans don't have complete confidence that they will be able to control who has access to their personal medical information.

I am proud to be a cosponsor of legislation to address these issues, including the consensus bill recently introduced by Mr. Condit. I believe his bill strikes a fair balance between protecting individual's rights and the legitimate access needs to encourage and assist medical research.

I believe H.R. 2470 fails to pass this "balanced" litmus test.

While complete analysis of the bill is not yet completed because it was only introduced three days ago, it already appears to lack basic and fundamental safeguards to protect individuals.

Among these is the loosely defined exception for "health care operations." As currently drafted in H.R. 2470, insurers could use an individual's health information for marketing purposes and insurance underwriting without consent by the individual.

Moreover, instead of creating a federal protection floor, this bill actually sets a ceiling and would preempt existing state laws and prevent states from passing laws to address their specific concerns.

Finally, this bill would prohibit the Secretary from taking additional steps in the future to address currently unforseen medical privacy protection issues.

Mr. Chairman I sincerely appreciate the efforts you and Mr. Greenwood have made in drafting this bill and I am disappointed that I am unable to support this bill in it's current form.

I look forward to working with the rest of the subcommittee Members on both sides to develop a fair and comprehensive bipartisan solution to this very bipartisan issue.

PREPARED STATEMENT OF HON. JOHN D. DINGELL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. Chairman, I want to begin by thanking you for scheduling this hearing. This is now our second hearing on the topic of medical records privacy. In view of the complex nature of the subject matter this is time well spent. All of us need to learn as much as we can about the uses and disclosures of personally identifiable medical information as they may occur in the modern, and I might add, ever changing, health care system. The proper use of such information can do great good for the patient, for research, and for public health and other legitimate purposes. But such information can also do great harm to the patient, to research, and other important purposes if used or disclosed improperly. Our job is to strike the appropriate balance between an individual's fundamental right to privacy and the need in certain circumstances for personally identifiable medical information to be used or disclosed by someone other than the patient.

I want to put the timing of this hearing and any further legislative action on medical records privacy in context. Much is made of the August 1999 deadline under the Health Insurance Portability and Accountability Act ("HIPAA"). The Secretary may begin the process of writing regulations if we do not enact legislation before then. She undoubtedly will need some period of time thereafter to complete the task. In sum, we need to move with alacrity, but there should be sufficient time to act under current law if we are serious about doing so, and there should be no need to extend the HIPAA deadline.

Mr. Chairman, today's hearing will hopefully inform us of key differences among competing approaches to medical records privacy legislation. I was pleased to join many of my colleagues, including Messrs. Condit, Waxman, Towns, and Markey in sponsoring H.R. 1941. I continue to believe that H.R. 1941 embodies sound medical records policies that include enforceable remedies and flexibility to meet future changes and challenges in this area. I see that my colleagues and good friends Messrs. Greenwood, Shays, Norwood, Burr, and Upton this week have also introduced a bill on this subject, H.R. 2470. I was disappointed to learn that this hearing has been captioned as dealing only with the Greenwood bill. Privacy is not a partisan issue.

Today, we will hear from two outstanding panels of witnesses. They include some of the leading experts on the subject of medical records privacy and I am anxious to learn from them.

Thank you.

Mr. BILIRAKIS. We will recess until after our vote. It will probably be about 15 minutes.

[Brief recess.]

Mr. BILIRAKIS. The hearing will come to order.

Panel I consists of Mr. John T. Nielsen, Senior Counsel and Director of Government Relations with Intermountain Health Care, Salt Lake City, Utah; Dr. Paul Tang, Medical Director of Clinical Informatics, Palo Alto Medical Clinic, Los Altos, California; Mr. Justin Pawlak of Harleysville, Pennsylvania; Dr. Paul S. Appelbaum, Professor and Chairman, Department of Psychiatry, University of Massachusetts Medical School; and Ms. Chai Feldblum, Director of Federal Legislation Clinic, Georgetown University Law Center.

Welcome. Your written statement is a part of the record, and we will set the clock at 5 minutes and ask you to try to hold to it as closely as you possibly can. We will start off with Mr. Nielsen. Please proceed, sir.

STATEMENTS OF JOHN T. NIELSEN, SENIOR COUNSEL AND DIRECTOR OF GOVERNMENT RELATIONS, INTERMOUNTAIN HEALTH CARE; PAUL C. TANG, MEDICAL DIRECTOR, CLINICAL INFORMATICS, PALO ALTO MEDICAL CLINIC; LINDA PAWLAK, PARENT; PAUL APPELBAUM, PROFESSOR AND CHAIR, DEPARTMENT OF PSYCHIATRY, UNIVERSITY OF MASSACHUSETTS MEDICAL SCHOOL, ON BEHALF OF THE AMERICAN PSYCHIATRIC ASSOCIATION; AND CHAI FELDBLUM, PROFESSOR OF LAW AND DIRECTOR, FEDERAL LEGISLATION CLINIC, GEORGETOWN UNIVERSITY LAW CENTER

Mr. NIELSEN. Thank you, Mr. Chairman, members of the committee. Good morning. My name is John T. Nielsen. I am Senior Counsel and Director of Government Relations for Intermountain Health Care. IHC, as it is called, is an integrated, not-for-profit healthcare system based in Salt Lake City. We serve the States of Utah, Idaho and Wyoming. The IHC system consists of 23 hospitals, over 400 employed positions and a large health plan division.

IHC employs 23,000 people who are keenly aware of their responsibility to safeguard personal health information, and we have invested considerable resources in order to develop effective protections and procedures to provide privacy protection for those that we serve.

IHC is pleased to strongly support the Medical Information Protection and Research Enhancement Act. We are pleased that H.R. 2470 reflects, among other things, six important key principles. First, H.R. 2470 wisely adopts uniform Federal confidentiality standards and preempts State authority in the areas covered by Federal legislation. Confidentiality legislation must ensure national uniformity and recognition of the increasingly complex and interstate nature of health care delivery in this country. I believe Mr. Greenwood has put it, as well as I have heard it in his opening statement.

Second, IHC supports H.R. 2470's statutory authorization approach. While it can certainly be argued that the practice of obtain-

ing signed authorization has value and merit, and indeed a study and a report by the Health Privacy Project at Georgetown University, of which I was part, recommends this approach, IHC has long maintained that the statutory authorization approach makes very good sense. This approach, combined with the bill's strong penalties for misuse, will allow for appropriate access to identifiable information while protecting patient confidentiality.

Mr. Greenwood's bill wisely allows the use of patient information only for expressly stated purposes which include treating, securing payment, conducting certain health care operations and other important purposes, including medical research, emergency services and public health.

Having said this and while IHC has certainly no objection to the approach taken in the bill, we would also have no objection to the more formal, signed authorization approach. After all, it is our current practice and may still be.

Third, H.R. 2470 applies Federal standards only to individually identifiable information, and this is the correct approach because patients have a legitimate expectation of privacy and because, perhaps more importantly, it creates a powerful incentive to encrypt, encode or otherwise anonymize patient health information.

Fourth, the act applies equally to all types of health information. All patient identifiable information is sensitive and should be afforded equal protections against inappropriate disclosure.

Fifth, the act rightly includes significant penalties for inappropriate use of protected information.

And last, sixth, it establishes new Federal safeguards to protect patient identifiable information. We are also pleased that the bill provides for a Federal right that patients may access, copy and request amendments to their medical records.

At IHC, in order to treat our patients and improve the health outcomes of the entire population we serve, we must be able to share information among our physicians, our hospitals and our health plans. IHC has developed state-of-the-art electronic medical records and common data bases to facilitate this communication, to make certain that our physicians have complete information when they treat patients. We have put into place an extensive array of enforceable confidentiality protections which we constantly improve and update.

We urge you to ensure that confidentiality legislation does not unintentionally prevent the creation of these common internal data bases or limit the type of data which can be shared within a health delivery system. Such action would severely limit a health care system's ability to measure and improve the health care outcomes of its patients.

Individually identifiable information and the ability to share it is absolutely integral to the IHC health care operations through which we seek to maximize the quality of patient health care delivered in our system. Health plans also play a major role in improving the health of our members. Health plans must be able to link information back to a specific individual in the event that a more effective treatment protocol or a previously unknown health risk is identified and to assist our members to manage their own health care.

For all of these reasons, we respectfully urge you to swiftly approve before the August recess the Medical Information Protection and Research Enhancement Act which we believe will establish important Federal standards to protect patient confidentiality which, at the same time, allows these important health-enhancing activities to continue.

Congress, not the Secretary, should set these standards in this critical area. We believe this bill will do just that. Thank you.

[The prepared statement of John T. Nielsen follows:]

PREPARED STATEMENT OF JOHN T. NIELSEN, SENIOR COUNSEL AND DIRECTOR OF GOVERNMENT RELATIONS, INTERMOUNTAIN HEALTH CARE

I. INTRODUCTION

My name is John T. Nielsen. I am Senior Counsel and Director of Government Relations at Intermountain Health Care (IHC). IHC is an integrated health care delivery system based in Salt Lake City and operating in the states of Utah, Idaho, and Wyoming. The IHC system includes 23 hospitals, 78 clinics and physician offices, 23 outpatient primary care centers, 16 home health agencies, and 400 employed physicians. Additionally, our system operates a large Health Plans Division with enrollment of 475,00 directly insured plus 430,000 who use our networks through other insurers.

IHC's 23,000 employees are keenly aware of their responsibility to safeguard personal health information and IHC has invested considerable resources in order to develop effective protections and procedures. IHC takes seriously its responsibility to use patient identifiable health information to optimize not only that patient's health, but the health of all patients in the IHC system.

II. IMPORTANCE OF FEDERAL LEGISLATION

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) directs Congress to enact federal privacy legislation by August 21, 1999. That deadline is little more than one month away. If Congress fails to act by August 21, 1999, the Department of Health and Human Services (HHS) is required to promulgate regulations on privacy protection by February 2000. IHC urges Congress to meet the HIPAA deadline and to enact strong federal standards which provide uniform patient confidentiality protections across the country. IHC is pleased to lend its strong and enthusiastic support to H.R. 2470, the *Medical Information Protection and Research Enhancement Act of 1999,* which is similar to S. 881, the *Medical Information Protection Act of 1999,* introduced by Senator Robert F. Bennett of Utah, which we also support.

IHC is committed to working with this Subcommittee and others in Congress toward passage of the Greenwood/Bennett bills. The approach adopted by these legislators strikes an appropriate balance between safeguarding patient identifiable health information and facilitating the coordination and delivery of high quality, network-based health care, such as that provided at IHC.

Indeed, striking the right balance is critical to IHC's efforts to deliver the best possible patient care. IHC has developed state-of-the-art electronic medical records and common databases which we use extensively not just for treatment and payment but for such fundamental quality enhancing activities as outcomes review, disease management, health promotion and quality assurance. Not only are these efforts essential to optimizing the health of our patients but many are in fact required by federal and state programs and regulations and by accreditation standards. It is vital that federal confidentiality legislation not impede the ability to optimize patient health through the use of identifiable health information.

III. IMPORTANCE OF NATIONALLY UNIFORM PATIENT CONFIDENTIALITY PROTECTIONS

The delivery of health care today is vastly different than even a decade ago. Health care delivery increasingly crosses state lines through health system mergers, telecommunications, contractual relationships and other mechanisms. Enactment of uniform federal confidentiality protections is critical as technology is increasingly used to enhance the quality of patient care and to maximize the outcomes of health care provided to our patients. Confidentiality legislation must ensure national uniformity in recognition of the increasingly complex and interstate nature of health care delivery in this country.

Health systems like IHC, which operate across state lines, would have enormous difficulty complying with different federal and state standards governing disclosure of protected health information. Individual state laws create confusion, errors and inefficiencies. The nation needs a common national standard for protection of confidentiality and privacy. Accordingly, strong federal preemption is vital. The *Medical Information Protection and Research Enhancement Act* rightly recognizes the importance of strong federal preemption.

IV. IHC USES PATIENT INFORMATION TO ENHANCE PATIENT CARE

IHC is committed to providing high quality health care to the communities it serves, regardless of ability to pay. IHC uses patient information to enhance patient care. A few specific examples of IHC's health care operations activities undertaken to improve health care outcomes are set forth below. The *Medical Information Protection and Research Enhancement Act* would facilitate the appropriate use of patient identifiable health information for these quality enhancing activities.

- *Improved timing of delivery of pre-operative antibiotics to prevent serious post-operative wound infections.* Our wound infection rate fell from 1.8 percent to 0.4 percent representing, at just one of our 23 hospitals, more than 50 patients per year who now do not suffer serious, potentially life-threatening infections. We also saved the cost of treating those infections, reducing health care costs by an estimated $750,000 per year at that one hospital.
- *Improved support for inpatient prescriptions.* A computerized order entry system warns physicians, at the time they place the order, of potential patient allergies and drug-drug interactions. It also calculates ideal dose levels, using the patient's age, weight, gender, and estimates of patient specific drug-absorption and excretion rates, based on laboratory values. That system has reduced adverse drug events (allergic reactions and drug overdoses) to less than one-third of their former level—significantly reducing the primary treatment-related risks that patients face while hospitalized.
- *Improved management of mechanical respirators for patients with acute respiratory distress syndrome (ARDS).* In the most seriously ill category of ARDS patients, mortality rates fell from more than 90 percent to less than 60 percent. Costs of care, per patient who lived, fell by about 25 percent.
- *Improved management of diabetic patients in an outpatient setting.* The proportion of patients managed to normal blood sugar levels (hemoglobin A1c < 7.0%) improved from less than 30 percent (typical for a general internal medicine practice) to more than 70 percent. Major studies of diabetes demonstrate that that shift in blood sugar control will translate to significantly less blindness, kidney failure, amputation, and death. Others indicate that it should reduce the costs of medical treatment for diabetic patients by about $1,000 per patient per year.
- *Improved treatment of community-acquired pneumonia.* By helping physicians more appropriately identify patients who needed hospitalization, choose appropriate initial antibiotics, and start antibiotic therapy quickly, we were able to reduce inpatient mortality rates by 26 percent. That translates to about 20 patients saved in the ten small rural IHC hospitals where we first worked on this aspect of care delivery. It also reduced treatment costs by more than 12 percent.
- *Accountability for health care delivery performance.* IHC has begun to assemble and report medical outcomes, patient satisfaction outcomes, and cost outcomes for major clinical care processes that make up more than 90 percent of our total care delivery activities. We aggregate and report those data at the level of individual physicians; practice groups (e.g., clinics); hospitals; regions; and for our entire system. We use the resulting reports to hold health care professionals and our system accountable for the care we deliver to our patients, and to set and achieve care improvement goals. We believe that this system will eventually allow IHC to accurately report our performance at a community, state and national level, to help individuals and groups make better choices in the United States' competitive health care marketplace.

Nearly all of IHC's 60-plus improvement projects, including the examples listed above, had to do with care delivery execution—consistently applying the best available current medical information—rather than the generation of new biomedical knowledge. Some of these initiatives directly improved medical outcomes for patients. Some primarily produced significant reductions in the cost of health care while demonstrably maintaining excellent medical outcomes, thus improving (albeit indirectly) affordability of and access to health care services. Many did both at once—improved medical outcomes while reducing costs.

All of these activities relied on information—not just information at the level of individual patients, but information on populations of patients. We use that popu-

lation-level information for operational care delivery—execution—not just "generation of new generalizable knowledge"—research. Medicine is inherently an information science. In general, the better objective data we have—with regard both to clinical theory, the information we use to care for a specific patient, and support to deliver the right care at the right time—the better diagnoses we can make, the better treatments we can offer and the better patient outcomes we can achieve.

Many recent, significant improvements in patient medical outcomes grew out of better health care delivery execution—that is, health care delivery operations. While the distinction between health care delivery operations and health research are clear at the extremes, it quickly turns to shades of grey at the center. No one has been able to produce a rigorous, functional definition to distinguish the two classes except at the extremes. It depends upon the intent of those examining the data.

National policy mistakes in this area—policies that inappropriately slow health care delivery, where other choices could have adequately protected patient confidentiality and privacy without raising functional barriers to care delivery execution—will be measured not just in increased health care costs, but in human lives. IHC urges this Subcommittee and others in Congress to work toward enactment of the *Medical Information Protection and Research Enhancement Act* because it recognizes the importance of patient identifiable health information and permits the appropriate flow of health information within a health care delivery system.

V. IHC RECOGNIZES THE CENTRAL IMPORTANCE OF THE CONFIDENTIALITY OF MEDICAL RECORDS AND HAS SET FORTH NUMEROUS INTERNAL PROCEDURES TO PROTECT CONFIDENTIALITY

IHC supports strong uniform federal confidentiality standards that buttress our health care delivery and clinical research work. Speaking through our community-based Board of Trustees, IHC has placed appropriate protection of patient confidentiality and privacy near the front of our institutional values. Those values complement a parallel mission to provide the best possible health maintenance and disease treatment to those who trust their care to our hands. On the eve of the 21st century, the best possible health maintenance and disease treatment is only possible when health care delivery operations use population-level patient data as well as individual patient data.

IHC uses enforceable corporate policy to maintain confidentiality (for health care professionals and employees, as well as patients) in those areas that are clearly health care delivery operations (for example, direct patient care delivery; billing for services; quality review of individual patient records, including such activities as mortality and morbidity conferences; resource planning, unit performance evaluation, quality improvement and disease management; and retrospective epidemiologic evaluations of program performance). The core of those policies and enforcement activities include:

- We require every employee, health care professional, researcher or volunteer to sign a confidentiality agreement stating that they will only look at or share information for the specific purpose of performing their health care delivery assignment on behalf of our patients.
- We require each new employee to undergo training with respect to IHC confidentiality policies. These policies are set forth in a draft manual, which already numbers more than 60 pages and represents more than five years of careful discussion and cross-testing.
- We impose consequences—including termination—for improper use or handling of confidential information.
- To the extent that we have implemented an electronic medical record, we are able to monitor access to patient records (an ability not present in the paper record). We use that system as one important means to monitor and enforce our confidentiality policy. In the near future, we will bring on-line the ability for any patient to review a list of every individual who has ever accessed their electronic medical record, for any purpose.
- We utilize software controls including warnings on front log-on screens, unique log-on passwords, and computerized audit trails. In the near future, we hope to be able to implement biometric log-on—where anatomic features (such as fingerprints) uniquely identify each computer user at each interaction.

VI. IRB REVIEW MUST NOT BE REQUIRED FOR HEALTH CARE DELIVERY OPERATIONS AND EXECUTION. IRB REVIEW IS NOT THE MOST EFFECTIVE WAY TO PROTECT PATIENT CONFIDENTIALITY.

IHC requires full Institutional Review Board (IRB) review, approval and on-going oversight for any research project that involves (1) any experimental therapy; (2) pa-

tient randomization among treatment options; or (3) patient contact for research purposes. Indeed, the IHC system has 12 IRBs, but we do not look to IRBs as our sole—or even our primary—means to protect confidentiality. Most of the risks to patient confidentiality come in day-to-day patient care, as physicians and nurses routinely access identifiable patient medical records, both paper and electronic, to deliver that care. Instead, we rely upon the extensive array of enforceable policies and procedures discussed above. In the same vein, a recent GAO Report affirms that IRBs "rely on organizational policies to ensure the confidentiality of information used in projects using personally identifiable medical information"[1] and that "the organizations... contacted have taken steps to limit access to personally identifiable information."[2]

If IRB review of each of these health care operations activities were required, many—if not most—of the operational care delivery and health outcome improvements described above could not function on a day-to-day basis. The volume of review would be staggering, far beyond the capacity of any reasonable system of individual review and follow-up oversight. While IHC has 12 fully functioning IRBs spread throughout our integrated health care delivery system, we do not look to these IRBs to protect the confidentiality of individually identifiable patient information for daily care delivery operations and execution. That protection arises, instead, from IHC-wide policy with administrative enforcement.

As the GAO report rightly recognizes "IRB review does not ensure the confidentiality of medical information used in research because the provisions of the Common Rule related to confidentiality have limitations."[3] Moreover, the report further acknowledges that "it is not clear that the current IRB-based system could accommodate more extensive review responsibilities."[4] If IRB review of quality improvement activities were required, our system's ability to conduct these fundamental quality-enhancing activities would be severely impeded.

IHC uses patient-identifiable health information to generate literally hundreds of operational analyses each day that improve the quality of health care. These quality improvement activities focus on both the processes of delivering care as well as on the outcomes of care. They include health promotion and disease prevention, disease management, outcomes evaluation for internal program management, and utilization management. As discussed above, IHC recognizes the vital importance of medical records confidentiality and has established numerous internal procedures to protect confidentiality.

Because it is so difficult to precisely define and distinguish between quality improvement-based internal operations and true clinical research activities, internal confidentiality policies and procedures accompanied by stiff penalties are far more effective in safeguarding patient confidentiality than mandating that quality improvement activities undergo IRB review. As the GAO Report acknowledges, the IRB process is already overburdened and is not designed to protect patient confidentiality. A care delivery system's ability to improve quality and deliver top-tier care would seriously be jeopardized if all of these activities were required to undergo IRB review.

IHC endorses the approach of the *Medical Information Protection and Research Enhancement Act* which acknowledges that requiring internal operations activities to undergo IRB review will not safeguard patient confidentiality. Instead, requiring a system-wide commitment and process with respect to safeguarding personal health information will better protect privacy.

VII. THE ROLE OF INSTITUTIONAL DATA REVIEW COMMITTEES

IHC's Information Security Committee recommends policy to IHC's Board of Trustees, and individually examines and acts upon all projects that fall into the definitional grey area between operations and research. The Information Security Committee reports directly to IHC's Board of Trustees. Its members include research scientists; experts in medical informatics; practicing clinicians; medical ethicists; a knowledgeable community member not associated with IHC or with other health care delivery or research; and senior managers from IHC's care delivery operations. As an extended quorum, all IRB chairpersons working within IHC also attend to discuss problems and recommend policy supporting IRB function

[1] U.S. General Accounting Office Report to Congressional Requesters, *Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections Is Limited,* GAO/HEHS-99-55, p16.
[2] *Id.* at 4.
[3] *Id.* at 3.
[4] *Id.* at 21.

throughout the IHC system. A full record of each meeting is generated and maintained.

IHC's Information Security Committee is an example of what the American Medical Informatics Association, in its recommendations on confidentiality protection when electronic medical records are used, calls a Data Review Committee. While structured very like an IRB, it adds an essential organizational element: a Data Review Committee is specifically charged to generate and enforce confidentiality policies within an organization, in addition to reviewing specific projects. An organization of IHC's size generates literally hundreds of operational analyses that access patient information every day. Especially when precise definitions are impossible, enforceable organization-level policy is far more effective in protecting confidentiality and privacy than is any attempt at individual review of such massive numbers of projects.

VIII. ELECTRONIC MEDICAL RECORDS ENHANCE INDIVIDUAL PATIENT CARE AND SIMULTANEOUSLY IMPROVE HEALTH CARE DELIVERY FOR ALL PATIENTS

A. Patients Must Not be Permitted to Opt Out of Quality Enhancing Activities

IHC uses an electronic medical record because of the significant improvements in medical outcomes and health care costs that that tool has allowed. Because it is such an essential part of daily operations, IHC cannot functionally allow patients to opt out of using our electronic medical record, without sacrificing (1) our ability to deliver excellent care to the individual involved and (2) our ability to provide good care to the rest of our patients. For example, our laboratory analyzers feed directly into our computer system. When IHC committed to that link, we not only significantly improved our ability to deliver excellent care to all of our patients, but also necessarily lost our ability to process blood laboratory tests without using the electronic medical record. Permitting patients to opt out would cripple IHC's ability to improve the health care quality of all of our patients. Even the loss of 3-4% of a patient population would greatly skew results. Moreover, from a functional perspective, given our use of electronic medical records, IHC could not logistically provide for patients to opt out of the various health promotion, disease management and other quality enhancing activities we routinely undertake.

B. Patient Requests to Alter their Medical Records

Because some providers like IHC are now using electronic medical records and other providers are increasingly using electronic medical records, IHC suggests that a patient's request to amend his or her medical record or a statement of a patient's disagreement with the content of a medical record be reflected in that medical record not by inclusion of the patient's entire written request or letter but by a notation or summary. The requirement in some legislative proposals for the inclusion of the full request or disagreement is impracticable given the increasing use of electronic medical records in the delivery of health care.

C. Patient Revocation of Authorization

Our physicians are legally and ethically bound to provide the best care they can for each patient. In order to do this, complete and accurate medical information is needed. If patients were permitted to deny consent for use of their medical records information, not only would their individual care be compromised, but ongoing efforts to improve health care quality and the validity and reliability of studies would be seriously jeopardized. Patients must not be empowered to pick and choose which information from their records should be made available to their physician and others with responsibility for caring for them. Instead, federal legislation should rely on severe penalties for misuse of information. The *Medical Information Protection and Research Enhancement Act* appropriately recognizes the necessity of ensuring that health care providers base decisions on the best possible information.

IX. STATUTORY AUTHORIZATION

The Secretary of Health and Human Services proposed a statutory authorization in her confidentiality recommendations. The National Association of Insurance Commissioners likewise incorporated this approach in their Model Act. A statutory authorization would authorize by law widely accepted uses of patient identifiable health information such as treatment, payment and the health care operations activities described above.

IHC is pleased that the *Medical Information Protection and Research Enhancement Act of 1999* includes a statutory authorization. This approach, combined with the strong penalties for misuse of information found in all of the legislative propos-

als on this issue, allows for appropriate access to identifiable health information while protecting patient confidentiality.

Ultimately, should Congress not adopt a statutory authorization, legislation must make clear that a signed patient authorization each time a provider and patient interact within a delivery system or network-based health plan is not required. Likewise, it is vitally important that the legislation allow health systems to engage in activities related to health promotion, disease management, quality assurance, utilization review, and related research without requiring separate patient authorization for each subsequent use of patient information. Such a requirement would be enormously burdensome for both providers and patients and, after the plans initial "consolidated authorization" is signed by the patient, would serve no additional purpose. IHC additionally urges that a health plan enrollee be permitted to sign one authorization form on behalf of that enrollee's covered dependents. Requiring each individual family member to sign a separate authorization form would be unwieldy at best, burdensome on the enrollee, and could result in the delay of needed care.

X. APPLICABILITY TO ALL HEALTH INFORMATION

Federal legislation should apply equally to all types of health information, including genetic information. This is important because all individually identifiable health information is sensitive and should be afforded the same protections against inappropriate disclosure.

XI. PENALTIES FOR MISUSE OF PROTECTED INFORMATION

All of the various legislative proposals include significant penalties for unauthorized use of patient identifiable health information. These are important to deter misuse of information. They should, however, be made consistent with the penalties included in HIPAA.

XII. CAUSE OF ACTION BY INDIVIDUALS

If Congress is able to meet the HIPAA deadline and enact confidentiality legislation, patients across the country will—for the first time—benefit from strong federal protections for patient identifiable information. Given the groundbreaking nature of this legislation and the significant criminal and civil penalties already provided for in the various legislative proposals, the inclusion of a private right of action is unnecessary. Moreover, it is our experience at IHC that breaches in the confidentiality of patient identifiable health information are not at all common. Additionally, inclusion of a private right of action would likely give rise to an entirely new plaintiff's bar, greatly increasing expensive and unpredictable private litigation. The penalty provisions in the various proposals, including the legislation before this Subcommittee, are already stringent; the addition of a cause of action is not merited.

XIII. LAW ENFORCEMENT

IHC feels that patient confidentiality legislation is an inappropriate venue for revision of probable cause and other standards now governing the access to patient records of law enforcement officials. Instead, confidentiality legislation should be law enforcement neutral. To the extent that confidentiality legislation touches on law enforcement's access to identifiable information, access should only be available after a request has been approved through a process that involves a neutral magistrate.

XIV. CLOSE

As an integrated health care delivery system, IHC is responsible for the health outcomes of the patients who seek care from our system. In order to treat our patients and improve the health outcomes of the entire population we serve, we must be able to share information among IHC corporate entities—our physicians, our hospitals, and our health plans. IHC has developed state-of-the-art electronic medical records and common databases to facilitate this communication and to make sure our physicians have complete information when treating patients. We have put in place an extensive array of enforceable confidentiality protections which we constantly improve and update.

IHC urges this Subcommittee to ensure that confidentiality legislation does not unintentionally prevent the creation of these common internal, operational databases or limit the type of data which can be shared within an integrated delivery system. Such action would severely limit a health system's ability to measure and improve the health outcomes it provides those who seek its services.

The outstanding health care our physicians, nurses, and others deliver through IHC's network-based system relies on the coordination of patient care and effective quality improvement activities. Individually identifiable health information is integral to IHC's health care operations, through which we seek to maximize the quality of patient care delivered in the IHC system. I urge you to swiftly approve—before the August recess—the *Medical Information Protection and Research Enhancement Act,* which will establish uniform federal standards to protect patient confidentiality while at the same time allowing these important activities to continue.

Mr. BILIRAKIS. Thank you very much, Mr. Nielsen .

Dr. Tang.

STATEMENT OF PAUL C. TANG

Mr. TANG. Thank you. Mr. Chairman, Mr. Greenwood, Members of the committee, thank you very much for permitting me to testify before you on this very important topic. My name is Paul Tang. I am a practicing internist and Medical Director of Clinical Informatics at Palo Alto Medical Clinic in California and Vice President of Epic Research Institute, working on computer-based patient record systems, or CPRs.

I am here because I have a passionate desire to provide the best quality care for my patients, and I think all caregivers have the legal and ethical obligation to protect the confidentiality of their patient's health data. In my mind, these two objectives are inextricably linked. I would like to begin by describing the status quo in medical recordkeeping, then explain a little bit on how CBR has improved that situation and to discuss how confidentiality legislation impacts quality of care.

First, the status quo. In an observational study I did a few years back at Stanford we found that in 81 percent of clinic visits physicians did not have all the information they needed to take care of their patients that day. In fact, on average, they were missing four pieces of information for each visit. This is not optimal. Unfortunately, neither is it atypical.

Regrettably, the situation in confidentiality is no better. If someone requests the medical record, it is an all or nothing phenomenon, and if the record can be found, and 30 percent of the time it can't be found, the request is free to look at any part of the record and no one will even know. It is this situation that makes it impossible for us to enforce confidentiality policies and to hold people accountable for their actions.

In 1991, the Institute of Medicine recommended that the United States adopt CPRs as the standard for medical record. They did this primarily because they thought it would improve the quality of care. In addition, it can increase our ability to protect the confidentiality of health information. For example, the CPR can limit access by a patient. So in contrast to common practice, where in a hospital almost anyone can look at a record, a CPR user can be limited only to those patients with which the user has a professional relationship.

Second, access to elements of a record can be restricted. So, for example, HIV test results can be marked as sensitive and restricted only to the ordering physician or the primary care physician.

Third, access to visits in mental health could be restricted to mental health providers.

Fourth and finally, and probably most importantly, all accesses to and updates of the record can be logged in audit trails and these audit trails can be analyzed to monitor and enforce confidentiality policies. Once again, in contrast to paper records, with the CPR, I can tell you who has access to your record and what they have looked at.

In short, a CPR gives us tools to increase the overall bar of protection of confidentiality for all patient data. I know that we all recognize that striking a balance between the needs of the caregiver and the need to protect information is difficult; and we all want to do the right thing, but as we work out the details of the legislation, I think we need to be careful about not letting good intentions interfere with good care.

For example, one approach to protecting patient data is to enumerate all the potentially sensitive personal data and to segregate that data. Unfortunately, to the extent that we are successful in hiding this information, we will undermine much of the benefit that computerizing records can provide us in the first place. In effect, we will have returned back to the status quo of having incomplete information for almost everybody.

An alternative approach and one that I would favor is to give physicians and patients the benefit of having all information when they are making decisions and at the same time raising the overall bar of protection for all data.

Finally, let me address the uniform confidentiality laws. Many provider organizations take care of patients across State borders. I think it would be confusing to patients and burdensome for providers to have to face State-by-State regulations. Like politics, health care is local, but I think our ethical and legal obligations to protect the confidentiality of patient data should be universal.

So, in summary, in my experience, CPRs can definitely enhance the quality of care, and they can definitely improve our ability to protect confidentiality of health data. However, we need balanced legislation in order to permit us to effectively use these tools to achieve the benefits I described and that the Institute of Medicine envisioned.

I think Mr. Greenwood's bill introduced this week is an example of balanced legislation that preserves the integrity of the record while assuring uniform protection for all. In short, we need confidentiality legislation to continuously improve the quality of health for all Americans. I thank you again for letting me testify before you, and I will be happy to answer any questions.

[The prepared statement of Paul C. Tang follows:]

PREPARED STATEMENT OF PAUL C. TANG, MEDICAL DIRECTOR OF CLINICAL INFORMATICS, PALO ALTO MEDICAL CLINIC

Mr. Chairman, Members of the Committee, thank you for the opportunity to testify on this very important topic—protecting the confidentiality of patient data. My name is Paul Tang. I am a practicing internist and Medical Director of Clinical Informatics at the Palo Alto Medical Clinic in California and Vice President of Epic Research Institute, working on computer-based patient record systems. I also serve on the Boards of the American Medical Informatics Association (AMIA), the Joint Healthcare Information Technology Alliance (JHITA), the Computer-based Patient Record Institute (CPRI), and the American College of Medical Informatics (ACMI).

I am here today because I have a passionate desire to provide high quality care for my patients and I firmly believe that all health care providers have an ethical

obligation to protect the confidentiality of their patients' health data. In my mind, these two objectives are inextricably linked. Consequently, your decisions regarding confidentiality legislation will directly affect the care that I can deliver.

I will begin by describing the inadequacies of the status quo in medical record-keeping, then speak briefly about the capabilities of computer-based patient records (CPRs) to address these needs, and conclude by discussing implications of confidentiality legislation on quality of care.

First, I need to tell you more about the status quo. In 1989, the Institute of Medicine initiated a study to look at ways of improving medical records in light of new information technology. During the committee deliberations, it was widely felt that the paper medical record left much to be desired. However, the literature did not contain empirical information about how broken the system really was. I later conducted a study at Stanford to gather the missing empirical data, and the results do not paint a pretty picture. When we observed physicians making patient care decisions in ambulatory care, we found that in 81 percent of the visits, physicians did not have all the information they needed in order to make decisions on their patients, even though they had the paper record 95% of the time. On average, physicians were missing 4 pieces of information during each visit. In one visit, a physician was missing 20 pieces of information. That is, physicians routinely have to choose between making a decision without the available information, rescheduling the patient for another visit in hopes that information will then become available, or repeating the test. Needless to say, none of these options is optimal. But, this is the standard of practice. In other words, we probably should be advising our patients that when they walk into a doctor's office they should expect that their physicians will be making decisions on their health care without all the available information.

I recall receiving a letter from a cardiologist pointing out the need for computer-based patient records in the hospital. One of his patients sustained a rare life-threatening side effect of a medication and was miraculously saved by an experimental treatment only to be given a medication later in her hospital stay to which she was allergic. Fortunately, by that time, she was alert and was able to refuse the medication. A CPR system could have warned the physician ordering the medication and prevented the near mishap.

Regrettably, the status quo for confidentiality is not much better. When a person requests a paper medical record, it is an all or nothing proposition. If the record can be found (30 percent of the time it cannot be found), the reader is free to look at any part of the record, and no one will know. The situation where a record and all of its contents are open to many eyes for any and all uses makes it impossible for us to enforce confidentiality policies and to hold people accountable for their actions. Like you, I find both these situations unacceptable—that doctors must routinely make decisions without all the relevant patient information and that we cannot adequately protect the confidentiality of patient data using paper records.

Fortunately, both of these problems can be dealt with by following the recommendations of the 1991 Institute of Medicine study on medical records, which concluded that the computer-based patient record is an essential technology for health care. Based on my past experience at Northwestern and my recent experience at Sutter Health, I can tell you that using a computer-based patient record (CPR) improves the quality of medical decisions and compliance with clinical guidelines. Let me cite a brief example of this. It is well documented that giving a flu vaccine to people 65 years and older reduces the mortality from flu-related complications by one-half, reduces flu-related hospital admissions by one-half, and reduces the cost of care by one-half. In effect, if you extrapolate these results, every time a flu vaccine is administered, it would save the country $117. Unfortunately, according to figures from the CDC and the literature, physicians routinely administer flu vaccines to approximately 50 percent of the eligible population. However, we and others have found that simple reminders provided by the computer at the time of a patient visit can dramatically increased the compliance with these simple, but effective guidelines. In a study we conducted at Northwestern, flu vaccine rates went up 78 percent for a group of physicians using a CPR compared to a control group in the same clinic that continued to use paper records.

In addition to helping physicians deliver better healthcare, a CPR can substantially improve our ability to protect the confidentiality of patient information. The guiding operational principle is that healthcare professionals should only have access to those data for which they have a professional need to know. The CPR has a number of capabilities to help ensure that this is the case. First, the CPR system can limit access by patient. In contrast to common practice where almost anyone in a hospital can access any patient record, a CPR can limit a user's access to those patients for which the user has a professional relationship. Second, a CPR can limit

the type of access based on the role of the user. For example, a physician may have complete access to a patient's record, but a clerk would only have limited access to administrative information about the patient. Third, access to specific elements of a record may be restricted. For example, an HIV test order and its results may be classified as sensitive and accessible only by the ordering physician or primary care provider. In addition, a visit where sensitive issues are discussed can be afforded similar protection by granting access only to the patient's physician. Fourth, access to visits in mental health departments could be restricted to mental health providers. Fifth, and probably the most important, all accesses to and updates of information in a CPR are logged and audit trails can be analyzed to monitor and enforce compliance with confidentiality laws and policies. Once again, in contrast to the paper record, with a CPR we can provide patients with a report of anyone who has accessed their record and what was examined. It is clear that using computer-based patient records gives us significant capability to raise the bar of protection for all confidential patient information.

What are the implications for confidentiality legislation? I think we all recognize that striking a balance between the information needs of physicians caring for patients and the need to control access to information is difficult and we all want to do the right thing. As the details of the legislation are worked out, however, we need to be careful not to let good intentions interfere with good care. For example, one approach to protection of patient data is to enumerate all potentially sensitive personal data and to segregate those data—rendering them more difficult to access. Unfortunately, to the extent that we succeed at hiding information, we will undermine much of the benefit of computerizing the record for the very people who care the most—the physician and the patient. In effect, we will have returned to the status quo that I described at the beginning of my testimony—that of incomplete information for almost everybody. An alternative approach, and one that I favor, is to give physicians and patients the benefit of making decisions based on information, but at the same time to raise the bar of confidentiality protection for all data using the capabilities of CPRs.

An analogy in patient care comes to mind. In the 1980s, health care providers wore gloves to protect them from blood-borne infectious diseases. This special precaution inadvertently became a marker for identifying patients with blood-borne diseases, which included AIDS patients. Consequently, a new policy called universal precautions was adopted where all patients are treated the same and gloves are worn anytime a health professional could potentially be exposed to blood. This approach accomplishes two things: it raises the general awareness among all caregivers about their everyday responsibility for preventing the spread of communicable diseases, and from the patient's perspective, everyone is treated the same; no one is inadvertently identified.

Likewise, I propose that instead of dissecting a patient's record into special pieces of information, which is likely to interfere with the care process, we should treat all patient information as highly confidential. Following my analogy to universal precautions, we would be preventing the spread of confidential data by treating all data the same. I would rather promote a new standard for confidentiality and hold providers to that higher standard for all data.

Under what conditions should provider organizations disclose identifiable patient information? The bills before Congress agree on treatment and payment reasons. What continues to be debated is the phrase "health care operations." While I am not in a position to enumerate every conceivable activity that could be covered, I can list some obvious examples of activities I think need to continue without separate disclosures. Among these activities are quality management, peer review, clinical teaching, disease management, quality reporting, and clinical research. What should not be allowed? Use of the information for any discriminatory practices. As lawmakers, you must draw the lines between what uses of health information should be permitted and which should not, probably in separate anti-discrimination laws. As a physician, however, I am concerned that encouraging patients to "opt out" of information systems (either by segregating information or through self-payment) can impair the quality of care not only for the individuals but for all of us.

Finally, let me address the issue of uniform confidentiality laws. Many provider organizations care for patients from multiple states. Implementing confidentiality regulations on a state-by-state basis would be confusing for patients and burdensome for providers. The standards which protect the confidentiality of health information should not depend upon geography. Like politics, health care may be local, but the ethical and legal obligation to protect confidentiality should be universal.

In my experience, using CPRs can definitely enhance the quality of care by helping physicians make informed decisions, while also substantially improving protection of confidentiality. However, we need balanced confidentiality legislation to effec-

tively use this tool to achieve the benefits that I described and that the Institute of Medicine envisioned. In summary, we need your legislation to continuously improve the health of all Americans.

Again, thank you for the opportunity to appear before you today. I will be happy to answer any questions.

Mr. BILIRAKIS. Thank your very much, Doctor.

Justin and Ms. Pawlak.

STATEMENT OF LINDA PAWLAK

Ms. PAWLAK. Good morning, Mr. Chairman and members of the subcommittee. My name is Linda Pawlak.

My son Justin has asthma. Justin was diagnosed with asthma approximately 8½ years ago. At the moment of his diagnosis, our lives changed. We lived in fear, as his illness pervaded every aspect of our lives. Because his illness was unpredictable, we placed restrictions on Justin and on our family in a vain attempt to circumvent an asthma attack, but because we were not appropriately managing his asthma, we were ill equipped to prevent these devastating attacks. The illness had complete control.

After approximately a year and half of suffering, Justin came under the care of a wonderful asthma specialist who taught us that asthma was a disease requiring diligent management, even when he wasn't ill. Justin's health improved. However, the big change didn't occur until we were told about, and began to participate in, an asthma management program called The Asthma and Allergy Support Center.

When Justin became a part of the program, he began logging onto a secured Web site on a daily basis. On his own personal Web page Justin began entering his daily peak flows, medications, symptoms and the potential triggers to which he had been exposed. Justin's doctor also logs onto his Web page on a daily basis to review Justin's progress. This sharing of information has allowed us and Dr. Bill to identify patterns and trends in Justin's daily management that would otherwise never have become apparent. These discoveries have led to better control of Justin's illness and a normalization of our lives. This sharing of data has also provided his physician with valuable information, information that could provide future improvement not only for Justin but for many of his other patients as well.

For many of his young years, Justin spoke of becoming a scientist so that he could find a cure for asthma. Since beginning on this management program, Justin no longer speaks of becoming a scientist in the future. He realizes that the information derived from his participation in this program could be the clue to crucial breakthroughs in asthma. He knows that he could be helping to find a cure for asthma today, tomorrow and well into the future.

As a mother, I am eternally grateful to the physician and staff members who identified Justin for potential participation in this program. It has changed our lives, just as it and other similar programs could change the lives of many others who bear the burden of ill health. Any legislation that would impede the use of information for research, that could cure this disease, or that would prevent others from learning about similar disease management programs, would be a terrible mistake. That is why we think Congressman Greenwood's bill is a step in the right direction.

If anyone is interested, we do have the computer here with us so that anyone who would care to can see what Justin does on a daily basis.

Thank you.

Mr. BILIRAKIS. Thank you, Ms. Pawlak. Justin, would you have anything you would like to add? Your mom has plenty of time left. You can do it.

Master PAWLAK. Not really. Mostly what she said in her speech is the same thing that I would say.

Mr. BILIRAKIS. She checked with you first, though, before she completed it. Thank you.

[The prepared statement of Linda Pawlak follows:]

PREPARED STATEMENT OF LINDA AND JUSTIN PAWLAK

Good morning Mr. Chairman and members of the Subcommittee. My name is Linda Pawlak. My son, Justin, has asthma. Justin was diagnosed with asthma approximately eight and a half years ago. At the moment of his diagnosis, our lives changed. We lived in fear, as his illness pervaded every aspect of our lives. Because his illness was unpredictable, we placed restrictions on Justin, and on our family, in a vain attempt to circumvent an asthma attack. But because we were not appropriately managing his asthma, we were ill equipped to prevent these devastating attacks. The illness had complete control.

After approximately a year and a half of suffering, Justin came under the care of a wonderful asthma specialist who taught us that asthma was a disease requiring diligent management, even when he wasn't ill. Justin's health improved. However, the big change didn't occur until we were told about, and began to participate in, an asthma management program called The Asthma and Allergy Support Center.

When Justin became a part of the program, he began logging onto a secured Website on a daily basis. On his own personal webpage, Justin began entering his daily peak flows, medications, symptoms, and the potential triggers to which he had been exposed. Justin's doctor also logs onto his webpage on a daily basis to review Justin's progress. This sharing of information has allowed us (and Dr. Bill) to identify patterns and trends in Justin's daily management that would otherwise never have become apparent. These discoveries have led to better control of Justin's illness and a normalization of our lives. This sharing of data has also provided his physician with valuable information, information that could provide future improvement not only for Justin, but for many of his other patients as well.

For many of his young years, Justin spoke of becoming a scientist so that he could find a cure for asthma. Since beginning on this management program, Justin no longer speaks of becoming a scientist in the future. He realizes that the information derived from his participation in this program could be the clue to crucial breakthroughs in asthma. He knows that he could be helping to find a cure for asthma today, tomorrow, and well into the future.

As a mother, I am eternally grateful to the physician and staff members who identified Justin for potential participation in this program. It has changed our lives, just as it (and other similar programs) could change the lives of many others who bear the burden of ill health. Any legislation that would impede the use of information for research, that could cure this disease, or that would prevent others from learning about similar disease management programs, would be a terrible mistake. That's why we think Congressman Greenwood's bill is a step in the right direction.

Mr. BILIRAKIS. Dr. Appelbaum.

STATEMENT OF PAUL APPELBAUM

Mr. APPELBAUM. Mr. Chairman, I am Paul Appelbaum, M.D., testifying on behalf of the American Psychiatric Association. I am Professor and Chair of the Department of Psychiatry at the University of Massachusetts Medical School, where I treat patients and oversee our department's biomedical and health services research, including our medical records-based research.

Mr. Chairman, ranking member Brown, I would like to thank you for the opportunity to testify today. I would also like to thank the members of the committee and Representatives Greenwood, Waxman and Markey, in particular, who have focused the committee's attention on medical records privacy by introducing comprehensive legislation.

Recently, several Commerce Committee members, including Mr. Markey and Mr. Whitfield, have raised major and, we believe, very important privacy concerns about the HCFA regulations, dubbed OASIS, and were helpful in dealing with that issue.

Based on our initial analysis of the proposed legislation, the APA is particularly concerned by H.R. 2470's lack of any consent process for patients, the preemption of stronger State privacy laws and the lack of essential privacy protections for patients in general and employees of corporations in particular. Our concerns are heightened by the fact that there are major features of this legislation which represent disturbing departures from most other legislative proposals in this area.

First, this legislation is the first Republican comprehensive medical records proposal which completely discards the time-tested approach of consent or authorization from patients before use or disclosure of medical records. If this legislation were enacted into law, it would mark a fundamental change in a key principle of patient privacy. Of course, to be meaningful, consent needs to be informed, voluntary and noncoerced, and many provisions of the legislation introduced by Representative Markey are valuable in this respect.

Second, unlike many of the other legislative proposals, H.R. 2470 does not contain specific prohibitions on employer access to medical records. We are gratified to hear Mr. Greenwood's statement that he intends to address this issue.

Third, we strongly urge reconsideration of H.R. 2470's blanket preemption of State medical records privacy laws. Again, the result of this preemption is that patients would lose important privacy protections that they now enjoy. Equally important, the States will lose the opportunity to enact stronger patient privacy laws in the future. In fact, at this point, 56 medical records confidentiality bills have passed at least one chamber of a State legislature this year. We support the approach in the Condit-Waxman-Markey bill which protects stronger State laws from preemption.

I would like to give you a concrete example to illustrate the unintended consequences that H.R. 2470 might have. I would like you to imagine that you are going into your doctor's office, and the doctor gives you a comprehensive physical examination. He takes your blood, he runs some lab tests. It all sounds harmless enough. After all, you have never signed anything giving permission for your personal information to be broadly used and disclosed. You were never told it would be used in such a way, and nothing was sent to you about that. But it will be extensively used, and nothing under 2470 would prevent that from happening.

Information from your medical records could be used for private research purposes without your consent or knowledge. Your age, sex, demographic information, psychiatric status and other information could be used for insurance underwriting and other broadly and vaguely defined health care operations purposes, again without

your consent or knowledge. Your medical records can be displayed to hundreds of medical students, nurses and other trainees because health care operations are defined to include health care education. Your medical records information and the medications you are taking can be revealed to pharmaceutical companies who may even contact you at home about taking their new product instead.

We have no problem with taking advantage of the considerable benefits of medical information and the new technologies that have been described here this morning. We are concerned that in that process we not sacrifice the privacy that Americans cherish.

I would be happy to respond to your particular questions during the question-and-answer period, either about 2470 or H.R. 10, to which Mr. Ganske referred earlier.

Thank you, Mr. Chairman. I look forward to working with the committee on this issue.

[The prepared statement of Paul Appelbaum follows:]

PREPARED STATEMENT OF PAUL APPFLBAUM ON BEHALF OF THE AMERICAN PSYCHIATRIC ASSOCIATIONINTRODUCTION

Mr. Chairman, I am Paul Appelbaum, M.D., testifying on behalf of the American Psychiatric Association (APA), a medical specialty society, representing more than 40,000 psychiatric physicians nationwide. I serve the APA as Vice-President and I am also Professor and Chair of the Department of Psychiatry at the University of Massachusetts Medical School. I would like to thank Chairman Bilirakis, Ranking Member Brown, and members of the Subcommittee for the opportunity to testify today.

Mr. Chairman, we greatly appreciate your interest in passing medical records privacy legislation. We also appreciate the work of Mr. Greenwood, Mr. Waxman, and Mr. Markey, as well as several Republican and Democrat members of the Committee who fought to improve the privacy provisions of HCFA's recent OASIS medical information regulation.

As changes in technology and health care delivery have outpaced the statutory, common law, and other protections that traditionally have ensured patient confidentiality, the level of confidentiality enjoyed by patients has eroded dramatically. I greatly appreciate your efforts to seize this valuable opportunity to protect and restore needed confidentiality protections.

The Need for Federal Legislation

I believe medical records confidentiality is one of the most important issues to come before the Subcommittee this year. Our ability to find a new job, earn a promotion, obtain insurance, our family and social relationships, the quality of health care, and medical research breakthroughs can all be enhanced or tragically jeopardized by medical records confidentiality legislation. Our medical record, when it relates to conditions as varied as high blood pressure, communicable diseases, Alzheimer's disease, mental illness and substance abuse, domestic violence, sexual assault information, terminal illnesses, HIV/AIDS, cancer, eating disorders, sexual function or reproductive health issues, as well as many other conditions, is highly sensitive.

But whether or not we are affected by these illnesses, medical records privacy issues affect us all. Today's comprehensive medical assessments and wellness questionnaires can contain questions about patients' sexual behavior, social relationships, state of mind, and psychiatric status—even if patients are not receiving medical treatment relating to these issues. The forms can also contain extensive personal and financial information.

The need for privacy legislation is compelling. In 1996, a federally appointed panel of experts, the National Committee on Vital and Health Statistics, stated that our country faces a "health privacy crisis." And across the political spectrum, broad support exists for action on this issue. Many conservatives, including Phyllis Schafly, have decried the "stealth assault on medical records." Likewise, liberals and civil libertarians have been fighting to secure basic protections to safeguard citizens from unjustified police seizure of their medical records. Finally, there has been bipartisan concern that led to the suspension of any implementation of a national patient identifier and the limitation of the Health Care Financing Administration's re-

cent medical information collection regulation, dubbed OASIS. Thus, it is clear that Americans of all political persuasions want to keep their personal medical information confidential. We hope that in the current debate on medical records privacy, bipartisan support can develop for enacting meaningful medical records privacy legislation into law.

Confidentiality is a Requirement for High Quality Medical Care

Common sense, the experience of physicians and patients, and research data all show that privacy is a critical component of quality health care. The sad fact is that the health care system has, on occasion, not earned the trust of patients, and many patients do not trust the system to keep their information confidential. In many cases, the result has been that physicians are not able to provide the best possible quality care nor reach many individuals in need of care.

Some patients refrain from seeking medical care or drop out of treatment in order to avoid any risk of disclosure. And some simply will not provide the full information necessary for successful treatment. At other times, physicians are approached by patients who ask us not to include certain information in their medical record for fear that it will be indiscriminately used or disclosed. The result of all these behaviors resulting from patients' reasonable concerns is unfortunate. More patients do not receive needed care and medical records' data that we need for many purposes, such as outcomes research, is regrettably tainted in ways that we often cannot measure.

The solution is not to take short cuts that will further deprive patients of their rights. Instead, we must enact into law meaningful medical records privacy legislation based on the voluntary informed consent of patients and reliance upon the fullest possible use of deidentified and aggregate patient data. In this way the full advantages of patient privacy as well as the benefits of new medical technology can be harnessed.

Informed, voluntary, and non-coerced patient consent prior to the use and disclosure of medical records should be the foundation of medical records confidentiality legislation. As a general principle, we believe that the American Medical Association's position—that patient consent should be required for disclosure of information in the medical record with narrowly drawn and infrequent exceptions permitted for overriding public health purposes—is eminently reasonable.

The Special Sensitivity of Mental Health Information and the U.S. Supreme Court's Jaffee Decision

Patients often refrain from entering psychiatric treatment because of concerns about confidentiality. Not only do patients refrain from telling family members and close friends the information they share with their therapist, but some may not even tell their family members that they are receiving mental health treatment. Often, if the information were disclosed to a spouse or an employer it might jeopardize their marriage or employment. But even the privacy protection afforded to psychotherapy notes has eroded so much in recent years that many psychiatrists and other mental health professionals have stopped taking notes or take only very abbreviated notes. Without the very highest level of confidentiality, patients receiving mental health services will be less likely to enter treatment and less likely to remain in treatment. Worse yet, if confidentiality is not protected, the treatment they receive will usually be less effective.

For these and other reasons, the U.S. Supreme Court recognized the special status of mental health information in its 1996 *Jaffee v. Redmond* decision. The court held that "Effective psychotherapy depends upon an atmosphere of confidence and trust—disclosure of confidential communications made during counseling sessions may cause embarrassment or disgrace. For this reason the mere possibility of disclosure may impede the development of the confidential relationship necessary for successful treatment."

It is also worth recognizing that the extent of mental illness is widespread. According to the World Health Organization mental illnesses account for four out of ten of the leading causes of disability. I urge members of this committee not only to protect the letter of the *Jaffee* decision but indeed to protect its spirit by including appropriate provisions in the legislation.

Provisions Needed in Congressional Legislation

It is not my intention to provide a detailed analysis of each bill before the Subcommittee but rather, I would like to recommend several key provisions that we believe should guide the Subcommittee in its deliberations, and we would be happy to provide the Committee with additional recommendations as well.

Preemption. I believe the most important medical records privacy issue before the Committee is to insure that stronger state medical records privacy laws are pre-

served and that states' ability to enact stronger medical records privacy laws are preserved. States have adopted valuable protections for patients, including laws limiting the disclosure of pharmacy records and laws blocking insurers' access to verbatim psychiatric notes. States are also actively considering numerous additional proposals. In fact, the National Council of State Legislatures estimates that a total of 56 medical records confidentiality bills have passed through at least one chamber of a state legislature. We must not block states' efforts to protect citizens' medical privacy. We recommend that the provisions in H.R. 2470 be modified to adopt a floor preemption approach as contained in the Condit-Waxman bill.

Consent. APA believes three principles should govern those sections of the legislation concerning authorization and consent for disclosure. *First,* patients themselves should decide whether or not personal health information is disclosed. Consent before use and disclosure of medical records is critically important and this time-tested approach should be preserved and strengthened in order to remain meaningful in the changing world of health care delivery. In general, whatever problems may now exist with confidentiality of health information are derived from our failure to observe this principle. No one is in a better position than patients themselves to identify sensitive information and to determine to whom it ought not to be revealed. Those who would alter this traditional approach have failed to justify such a radical change.

Second, identifiable personal health information should be released only when deidentified data is inadequate for the purpose at hand. *Third,* even when consent has been obtained, disclosure should be limited to the least amount of personal health information necessary for the purpose at hand. This is consistent with our recognition of the importance of protecting medical privacy.

These principles have implications for some of the major policy questions regarding authorization of disclosure. For patients to retain meaningful control over personal health information, prospective consent for routine disclosures of identifiable information should be largely limited to information needed for treatment and payment purposes. Other health care operations can usually be accomplished with deidentified data. With such a provision, a strong incentive will exist for the use and further enhancement of technology to perform a wide array of administrative functions.

We are extremely concerned because H.R. 2470 reverses the time-tested principle of consent before disclosure. Many patients will not even be aware that their most sensitive information is being used or disclosed for a host of purposes far beyond treating their illness or paying for the service. Were this legislation to be enacted into law, we fear that gradually patients would learn how little control they have over disclosure of their most personal information. As a result, many patients would refrain from providing their physician with the full information about their medical condition or they would refrain from obtaining care.

Unlike each one of the other three Republican bills before the Congress, i.e. Senate bills introduced by Senator Robert Bennett (R-UT) and Senator James Jeffords (R-VT) and a House bill introduced by Representative Chris Shays (R-CT) the Greenwood bill eliminates the principle of current law requiring consent before disclosure. We strongly urge the Committee to adopt an alternative approach based on the aforementioned principles.

Health Care Operations. In particular, the APA is also very concerned by the definition of "operations" in H.R. 2470. Entities providing health care can use and disclose this information for "operations" purposes, i.e. many purposes not directly related to treating a patient or performing payment or reimbursement functions. Some of the terms that are used to define "operations" are quite vague and broad and could endanger patient privacy. Do we really want to permit patients to be terminated from their health care coverage because they don't want their personal records to be used for largely commercial functions that can be performed with aggregate data?

Employee Protections. Millions and millions of Americans have great concern about the threat to confidentiality of their medical records due to employer access. Whether it is idle gossip by individuals with access to medical records, employer review of identifiable medical records data, or supervisors' inappropriate interest in the personal lives of their employees we must protect employees right to medical records privacy. Wouldn't most people want to decide if anyone in their company, not to mention their supervisor, would know if they obtained medical care from a psychiatrist, from a cardiologist, from an obstetrician/gynecologist, or from an oncologist?

We believe that the strong, explicit protections are needed in this area such as the provisions included in several bills, most notably those introduced by Senator Robert Bennett (R-UT) and separate legislation introduced by Representatives Gary

Condit (D-CA) and Henry Waxman (D-CA). Loopholes in H.R. 2470's definition of "health plan" and "protected health information" also need to be closed so that employees can be assured of adequate medical privacy protections.

Needed Protections for Particularly Sensitive Medical Information. As indicated above, especially sensitive information, including mental health information needs to receive a very high level of protection. Indeed, the U.S. Supreme Court itself in its *Jaffee* decision recognized that additional privacy protections, above and beyond those afforded to other health information, are needed to insure effective psychiatric care. APA believes that in order to promote high quality medical care and patient privacy, the Congress should pass legislation that provides a level of protection high enough so that no class of information needs additional protections. However, in the event that the Congress proceeds with legislation that does not meet this test, strong additional privacy protections will clearly be needed for mental health information.

Medical Records Provisions of H.R. 10, Financial Services Modernization Legislation.

Any discussion of current medical records legislation involving the House Commerce Committee must also focus on the damaging medical records provisions included in H.R. 10, the Financial Services Modernization bill soon to be discussed before a House-Senate Conference Committee. Despite the good intentions that led to the adoption of these provisions, we remain extremely concerned that this legislation will hurt, not help, the cause of medical records privacy, both because of the legislation's likely preemption of state privacy laws and its lack of basic medical records privacy provisions contained in all the medical records privacy legislation before the Congress.

We attach a letter signed by 40 physician, provider, patient, and other organizations opposing these provisions. Groups opposing these provisions include the American Medical Association, the American Association of Family Physicians, the American Lung Association, the Service Employees International Union, and the American Federation of State, County and Municipal Employees.*Conclusion*

As physicians, we take an oath first stated by Hippocrates that, "Whatsoever things I see or hear concerning the life of men, in my attendance on the sick—I will keep silence thereon, counting such things to be as sacred secrets." In order to make sure that doctor-patient confidentiality continues to protect patients in the new millennium, I strongly urge the Committee to provide the highest possible level of confidentiality in your legislation.

We thank you for this opportunity to testify, and we look forward to working with the Committee on these important issues.

NOTE: Over 40 groups signed on to this letter including the American Medical Association, American Lung Association, and Service Employees International Union.

June 29, 1999

MEMBER OF CONGRESS
House of Representatives
Washington, DC 20515

Medical Records Provisions of H.R. 10 Undermine Patient Privacy

DEAR REPRESENTATIVE: The undersigned physician, provider, patient, and other national organizations strongly support medical records confidentiality not only from a personal privacy perspective, but also because of the critical importance of patient privacy for high quality medical care. We greatly appreciate the well-intentioned efforts of the many members that have resulted in the medical records privacy provisions of H.R. 10. Nevertheless, we have both serious procedural and substantive concerns about these provisions and urge that they be deleted from the bill.

We are particularly concerned because Section 351 of the bill would allow the use and disclosure of medical records information without the consent of the patient in extraordinarily broad circumstances. To give just two examples, law enforcement entities would enjoy virtually unfettered access to medical records and insurance companies could review individual medical records in performing marketing studies. The list of entities that could obtain medical records is also extensive. Why should life insurers, auto insurers, and even insurers providing travel cancellation insurance be able to routinely access patients' entire medical records without patient consent or even knowledge?

To complicate matters further, the legislation establishes no limitations on subsequent disclosures of medical records to non-affiliated entities. Once a disclosure has

occurred, there is no limitation on the types of disclosures that the recipient of this information may make. Thus, if an insurer contracts out a certain authorized service to a bill collection agency or an administrative support company, nothing in the legislation would prevent these organizations from disclosing or selling the information for a host of inappropriate purposes far beyond any legitimate health use.

The legislation lacks basic protections included in all the major confidentiality bills before the Congress. The legislation lacks specific requirements for physical, technical, and administrative safeguards to prevent unintended disclosures of medical records. Nor does the legislation encourage the use of deidentified medical records or insure that patients will receive notice of the confidentiality, use, and disclosure practices of the insurance companies.

Confidentiality between the doctor or other health care professional and the patient is an essential component of high quality health, and particularly mental health, care. Unfortunately, the medical records confidentiality provisions in H.R. 10 will deter many patients from seeking needed health care and deter patients from making a full and frank disclosure of critical information needed for their treatment.

We also have numerous procedural concerns. Because the Senate HELP Committee has not yet been able to report out comprehensive medical records privacy provisions, H.R. 10's provisions, intended as a temporary measure until comprehensive legislation is enacted into law, could now become long-lasting. This is extremely troublesome because H.R. 10 is designed to address only certain narrow aspects of medical records privacy and leaves key issues unresolved. We are deeply concerned that passage of H.R. 10's current medical records privacy language has the potential to undermine enactment of comprehensive medical records privacy legislation.

Thank you for considering these important issues. For further information, please contact William Bruno of the American Psychiatric Association at (202) 682-6194.

Sincerely,

AMERICAN PSYCHIATRIC ASSOCIATION; AMERICAN COLLEGE OF OCCUPATIONAL AND ENVIRONMENTAL MEDICINE; AMERICAN ACADEMY OF CHILD AND ADOLESCENT PSYCHIATRY; AMERICAN ACADEMY OF FAMILY PHYSICIANS; AMERICAN ASSOCIATION OF OCCUPATIONAL HEALTH NURSES, INC; AMERICAN ASSOCIATION FOR PSYCHOSOCIAL REHABILITATION; AMERICAN COLLEGE OF PHYSICIANS—AMERICAN SOCIETY OF INTERNAL MEDICINE; AMERICAN COLLEGE OF SURGEONS; AMERICAN COUNSELING ASSOCIATION; AMERICAN FAMILY ASSOCIATION; AMERICAN FAMILY FOUNDATION; AMERICAN FEDERATION OF STATE, COUNTY, AND MUNICIPAL EMPLOYEES; AMERICAN LUNG ASSOCIATION; AMERICAN MEDICAL ASSOCIATION; AMERICAN OCCUPATIONAL THERAPY ASSOCIATION; AMERICAN OSTEOPATHIC ASSOCIATION; AMERICAN PSYCHOANALYTIC ASSOCIATION; AMERICAN PSYCHOLOGICAL ASSOCIATION; AMERICAN SOCIETY FOR GASTROINTESTINAL ENDOSCOPY; AMERICAN SOCIETY OF CLINICAL PSYCHOPHARMACOLOGY; AMERICAN SOCIETY OF CATARACT AND REFRACTIVE SURGERY; AMERICAN SOCIETY OF PLASTIC AND RECONSTRUCTIVE SURGEONS; AMERICAN THORACIC SOCIETY; ANXIETY DISORDERS ASSOCIATION OF AMERICA; ASSOCIATION FOR AMBULATORY BEHAVIORAL HEALTH; ASSOCIATION FOR THE ADVANCEMENT OF PSYCHOLOGY; BAZELON CENTER FOR MENTAL HEALTH LAW; CORPORATION FOR THE ADVANCEMENT OF PSYCHIATRY; FEDERATION OF BEHAVIORAL, PSYCHOLOGICAL AND COGNITIVE SCIENCES; INFECTIOUS DISEASE SOCIETY; INTERNATIONAL ASSOCIATION OF PSYCHOSOCIAL REHABILITATION SERVICES; NATIONAL ASSOCIATION OF DEVELOPMENTAL DISABILITIES COUNCILS; NATIONAL ASSOCIATION OF PSYCHIATRIC TREATMENT CENTERS FOR CHILDREN; NATIONAL ASSOCIATION OF SOCIAL WORKERS; NATIONAL ASSOCIATION OF STATE MENTAL HEALTH PROGRAM DIRECTORS; NATIONAL COUNCIL FOR COMMUNITY BEHAVIORAL HEALTHCARE; NATIONAL DEPRESSIVE AND MANIC DEPRESSIVE ASSOCIATION; NATIONAL FOUNDATION FOR DEPRESSIVE ILLNESS; NATIONAL MENTAL HEALTH ASSOCIATION; RENAL PHYSICIANS ASSOCIATION; AND SERVICE EMPLOYEES INTERNATIONAL UNION.

Mr. BILIRAKIS. Thank you very much, Doctor.

Ms. Feldblum. I am sorry, did I mess up your name?

STATEMENT OF CHAI FELDBLUM

Ms. FELDBLUM. Oh, if you did, you would join a long list. Actually, it is the first name that people have trouble with.

My name is Chai Feldblum. I am a law professor at Georgetown Law School, and I created and run a Federal Legislation Clinic where I teach students what I call the art of legislative lawyering,

which is the art of merging politics and law. And I will second all the comments some of you have made about this bill. We have been working on this for 6 years, and I can tell you we have had hundreds of quality teaching moments on his bill because of how complicated it is.

One of the pro bono clients of the clinic is the Privacy Working Group of the Consortium for Citizens With Disabilities, that is, it is the coalition of people with disabilities. We represent the asthma groups, the diabetes groups, epilepsy, cancer, et cetera.

For people with disabilities, having an effective health care system is key. We have never seen this as balancing privacy against an effective health care system. It has always been for us in the 6 years we have been working, how do we enhance the privacy protections in the health care system so people have trust in the system so that it works well. That has always been our goal.

We are also a very practical group. We know we have a particular approach to have effective privacy and effective health care system, but industry stakeholders might have a different approach. So we have spent a significant amount of time in two forums finding out what are the concerns of industry stakeholders so that the description, Mr. Greenwood, you gave of the health care system you would like to see fits the language that is in the bill that you have authored. That is our goal in this clinic, that the rhetoric of the intention fits the actual words that are used.

My assessment in reading 2470 and my written testimony is in significant detail, excruciating to some, welcome to others; I will give you only the highlights here. What I see in 2470 is absolutely the intention to achieve the goals that you have described. A few areas where the legal words are simply not going to achieve that result—I don't think any of these are insurmountable.

I think some are more difficult than others. I think private right of action and preemption will be more difficult than others because of policy, but some of the other things that I think are problematic in the bill, I don't think are insurmountable. Why don't I? Because we have been working with industry, not just here on the House side, but over on the Senate side, outside of the legislative process.

The Health Privacy Working Group that Mr. Nielsen referred to—and Mr. Chairman, I would like to introduce that report into the record if I may.

Mr. BILIRAKIS. Without objection.

[The report follows:]

HEALTH
PRIVACY
PROJECT

INSTITUTE FOR HEALTH CARE
RESEARCH AND POLICY
GEORGETOWN UNIVERSITY

principles FOR HEALTH PRIVACY

A REPORT OF THE
HEALTH PRIVACY WORKING GROUP

WITH SUPPORT FROM
THE ROBERT WOOD
JOHNSON FOUNDATION

THE HEALTH PRIVACY WORKING GROUP

The Health Privacy Working Group is an initiative of the Health Privacy Project of Georgetown University's Institute for Health Care Research and Policy. The Working Group is funded through a generous grant from the Robert Wood Johnson Foundation.

The Working Group is staffed by Janlori Goldman, Director, and Zoe Hudson, Policy Analyst, Health Privacy Project. The Project wishes to thank the Robert Wood Johnson Foundation, in particular Judith Whang, who recognized the importance of this challenge; the Glen Eagles Foundation and the Trellis Fund, most notably Betsy Frampton and Hope Gleicher, who saw the promise in this Project; Andy Burness, Linda Loranger, and the rest of the staff of Burness Communications for their guidance throughout the process; Scott Sanders of High Noon Communications, Audrey Denson of Denson Design, and Mike Heffner of 202 Design for their keen design skills; and our colleagues at the Institute for Health Care Research and Policy.

Our deep appreciation goes to the individual members of the Working Group, who dedicated themselves over the past year to this extremely daunting—and we hope just as valuable—endeavor. As Chair, Dr. Bernard Lo brought to bear his vast knowledge and talents as doctor, ethicist, teacher, writer, listener, and refiner, all of which made this possible.

MEMBERS

Chair
Bernard Lo
Director, Program in Medical Ethics
University of California San Francisco

Paul Clayton
Professor of Medical Informatics
Columbia Presbyterian Medical Center and
Intermountain Health Care

Jeff Crowley
Chair, Privacy Working Group
Consortium for Citizens with Disabilities and
Deputy Executive Director for Programs
National Association of People with AIDS

John Glaser
Vice President and Chief Information Officer
Partners HealthCare System, Inc.

Nan Hunter
Professor of Law
Brooklyn Law School

Shannah Koss
Healthcare Security and Government
Programs Executive
IBM

Chris Koyanagi
Policy Director
Bazelon Center for Mental Health Law

John Nielsen
Senior Counsel and Director of Government
Relations
Intermountain Health Care

Linda Shelton
Policy Director
National Committee for Quality Assurance

Margaret VanAmringe
Vice President for External Affairs
Joint Commission on Accreditation of
Healthcare Organizations

HEALTH PRIVACY WORKING GROUP
BEST PRINCIPLES FOR HEALTH PRIVACY

EXECUTIVE SUMMARY 3

BACKGROUND AND OVERVIEW 8

Privacy-Protective Behavior 8
Benefits and Risks of Technology 9
National Attention to Health Privacy 10
Formation of the Health Privacy
Working Group 12
Best Principles for Health Privacy 12
Scope of Principles 13

BEST PRINCIPLES

Principle #1: Non-Identifiable Information 15
Principle #2: Privacy Protections Follow the Data . . .17
Principle #3: Right of Access 18
Principle #4: Notice 19
Principle #5: Safeguards 20
Principle #6: Authorization 22
Principle #7: Organizational Policies 34
Principle #8: Research 36
Principle #9: Law Enforcement 39
Principle #10: Discrimination 40
Principle #11: Remedies 41

Definitions 42

APPENDICES

Appendix A: Resources 43
Appendix B: Member Biographies 46
Appendix C: Staff Biographies 51

EXECUTIVE SUMMARY

Executive Summary

Privacy and confidentiality have long been recognized as essential elements of the doctor-patient relationship. Also essential to optimal care is the compilation of a complete medical record. But that same record is used for a wide variety of purposes—including insurance functions, coordination of care, and research. The long-standing friction between these two goals—patient privacy and access to information for legitimate purposes—has been heightened by the transition to electronic health information and a push toward integrated information in support of integrated health care delivery and health data networks. While these developments are intended to improve health care, they also raise many questions about the role of privacy in the health care environment.

Recent polls demonstrate that the public has significant concern about the lack of privacy protection for their medical records and that it can impact how they engage with health care providers. In order to protect their privacy, some patients lie or withhold information from their providers; pay out-of-pocket for care; see multiple providers to avoid the creation of a consolidated record; or sometimes avoid care altogether. Such "privacy-protective" behavior can compromise both individual care and public health initiatives.

The public has some reason to be concerned. Today, there is little consistency in approaches to patient confidentiality and no national standards or policies on patient confidentiality. The 1996 Health Insurance Portability and Accountability Act provides that if Congress fails to enact comprehensive health privacy legislation by August 1999, the Secretary of Health and Human Services must issue regulations. Therefore, either through legislation, government regulation, or self-regulation, there will be significant developments with regard to health privacy in the next two years.

3

What has been missing from the debate is a consensus document that offers policy recommendations regarding how best to protect patient confidentiality. To fill this void, the Health Privacy Project, with funding from the Robert Wood Johnson Foundation, created the Health Privacy Working Group in June 1998. Its mission was to achieve common ground on "best principles" for health privacy, while identifying a range of options for putting those principles into practice. The Working Group is comprised of diverse stakeholders, including: disability and mental health advocates; health plans; providers; employers; standards and accreditation representatives; and experts in public health, medical ethics, information systems, and health policy.

The Working Group spent the past year crafting a consensus document that reflects "best principles" for health privacy. This report outlines the 11 principles to which the Working Group agreed and details the rationale behind the recommendations.

Best Principles for Health Privacy

The principles represent significant compromises between Working Group members and should be seen as a framework that aims to accommodate the various information needs of diverse interest groups. The principles are designed to establish a baseline of

Executive Summary

protections that should be considered when implementing comprehensive patient privacy policies and practices.

The Working Group adopted the following 11 principles. Because these principles are intended to establish a comprehensive framework, they should be read and implemented as a whole.

1. **For all uses and disclosures of health information, health care organizations should remove personal identifiers to the fullest extent possible, consistent with maintaining the usefulness of the information.**

Generally, the use and disclosure of information that does not identify individuals does not compromise patient confidentiality. As such, the use and disclosure of non-identifiable health information should "fall outside" the scope of policies that govern personally identifiable health information. Health care organizations will need to take into consideration the practicality and cost of using and disclosing non-identifiable information. Ultimately, through the creation and use of non-identifiable health information, more people can have more information, without compromising patient confidentiality.

2. **Privacy protections should follow the data.**

All recipients of health information should be bound by all the protections and limitations attached to the data at the initial point of collection. Recipients of health information can use or disclose personally identifiable health information only within the limits of existing authorizations. Any further uses or disclosures require specific, voluntary patient authorization.

3. **An individual should have the right to access his or her own health information and the right to supplement such information.**

All patients should be allowed to copy their records and to supplement them if necessary. But supplementation should not be implied to mean "deletion" or "alteration" of the medical record. Furthermore, data holders may charge a reasonable fee for copying the records, but they cannot refuse inspection of the records simply because they are owed money by the individual requesting inspection.

In certain cases, patients may be denied access to their medical records. Such instances include if the disclosure could endanger the life or physical safety of an individual; if the information identifies a confidential source; if the information was compiled in connection with a fraud or criminal investigation that is not yet complete; or if the information was collected as part of a clinical trial that is not yet complete and the patient was notified in advance about his or her rights to access information.

4. Individuals should be given notice about the use and disclosure of their health information and their rights with regard to that information.

The notice should tell the patient how information will be collected and compiled, how the collecting organization will use or disclose the information, what information the patient can inspect and copy, steps the patient can take to limit access, and any consequences the patient may face by refusing to authorize disclosure of information.

5. Health care organizations should implement security safeguards for the storage, use, and disclosure of health information.

Security safeguards consistent with the Secretary of Health and Human Service's standards, whether technological or administrative, should be developed to protect health information from unauthorized use or disclosure and should be appropriate for use with electronic and paper records. Any safeguards should recognize the trade-off between availability and confidentiality and should be tailored to meet needs as organizations adopt more sophisticated technologies.

6. Personally identifiable health information should not be disclosed without patient authorization, except in limited circumstances. Health care organizations should provide patients with certain choices about the use and disclosure of their health information.

Patient authorization should be obtained prior to disclosure of any health information. But, at the same time, some patient information needs to be shared for treatment, payment, and core business functions. With this in mind, the Working Group recommends a two-tiered approach to patient authorization.

The authorization structure allows for a health care organization to obtain a single, one-time authorization for core activities that are considered necessary or routine. These activities are directly tied to treatment, payment, and necessary business functions in keeping with medical ethics. The health care organization may condition the delivery of care—identified as Tier One—or payment for care upon receiving authorization for these activities, which can be obtained at the point of enrollment or at the time of treatment.

Any activities that fall outside this core group (sometimes commonly referred to as uses) must be authorized separately by the patient and fall under Tier Two authorization. The patient can refuse authorization for these activities without facing any adverse consequences. Activities in this category include, but are not limited to:

- purposes of marketing;
- disclosure of psychotherapy notes;
- disclosure of personally identifiable health information to an employer, except where necessary to provide or pay for care;
- disclosure of personally identifiable health information outside the health care treatment entity that collected the information, if other Tier One authorization(s) do not apply;

Executive Summary

and
- disclosure of personally identifiable health information, if adequate notice has not been given at the point of the initial authorization.

The Working Group identified a limited number of circumstances in which personally identifiable health information may be disclosed without patient authorization. These include:
- when information is required by law, such as for public health reporting;
- for oversight purposes, such as in fraud and abuse investigations;
- when compelled by a court order or warrant; and
- for research, as described in Principle 8 below.

7. Health care organizations should establish policies and review procedures regarding the collection, use, and disclosure of health information.

An organization's confidentiality policies and procedures should be coherent, tying together authorization requirements, notice given to patients, safeguards, and procedures for accessing personally identifiable health information. Organizations should also establish review processes that ensure a degree of accountability for decisions about the use and disclosure of personally identifiable health information. During such a process organizations might, for example, wish to determine routine procedures and special procedures for some areas of health care where medical information is considered highly sensitive to the patient.

8. Health care organizations should use an objective and balanced process to review the use and disclosure of personally identifiable health information for research.

For some areas of research, it is not always practical to obtain informed consent and, in some cases, a consent requirement could bias results. Recognizing this, the Working Group advises that patient authorization should not always be required for research. However, any waivers of informed consent should only be granted through an objective and balanced process.

Currently, any federally funded research is subject to the "Common Rule," where an Institutional Review Board (IRB) is required to make a determination about the need for informed consent. An IRB can choose to give a researcher access to personally identifiable health information with or without informed consent. But some research falls outside the scope of federal regulations. In such circumstances, health care organizations should use a balanced and objective process before granting researchers access to personally identifiable health information.

9. Health care organizations should not disclose personally identifiable health information to law enforcement officials, absent a compulsory legal process, such as a warrant or court order.

Best Principles for Health Privacy

Federal privacy laws generally require that some form of compulsory legal process, based on a standard of proof, be presented in order to

disclose to law enforcement officers. Law enforcement access to health information should be held to similar standards. In some instances, however, government officials may access health information with legal process for the purposes of health care oversight. In these instances, the information obtained should not be used against the individual in an action unrelated to the oversight or enforcement of law nor should the information be re-disclosed, including to another law enforcement agency, except in conformance with the privacy protections that have attached to the data.

10. Health privacy protections should be implemented in such a way as to enhance existing laws prohibiting discrimination.

Currently, there are state and federal laws that prohibit discrimination on the basis of a person's health status in areas such as employment or insurance underwriting. Confidentiality policies should be implemented in such a way as to enhance and complement these protections. In effect, privacy can serve as the first line of defense against discrimination, creating a more comprehensive framework of protection.

11. Strong and effective remedies for violations of privacy protections should be established.

Remedies should be available for internal and external violations of confidentiality. Health care organizations should also establish appropriate employee training, sanctions, and disciplinary measures for employees and contractors who violate confidentiality policies.

The 11 principles outlined above focus on information gathered in the context of providing patient care and are written to establish a broad framework for the use and disclosure of health information. Although the Working Group recognizes that the need for privacy protections in other areas is no less urgent, this consensus document does not address the following areas:

- special considerations about the needs of minors;
- information that locates an individual in a particular health care organization (sometimes referred to as "directory information");
- information provided to spouses, dependents, and other next of kin;
- public health reporting;
- fraud and abuse investigations; and
- the appropriate relationship between state and federal law.

These 11 principles are designed to serve as a baseline for establishing patient privacy protections. While we all agree that health information, used in the right hands and with the right safeguards, can lead to improved health and advances in research, this information should not be used with disregard for patient privacy. Patients need to know that adequate protections are in place to protect their health information. Our hope is that these principles will go a long way towards establishing appropriate protections and, in the process, help build public trust and confidence in our health care system.

Background and Overview

BACKGROUND AND OVERVIEW

Confidentiality has long has been an essential element of the relationship between patients and health care professionals. But contrary to popular belief, the information people share with their doctors has never remained completely private—initiatives to improve individual and community health depend on accumulation of, and access to, medical records and other patient information.

The often uneasy interplay between protecting privacy and improving quality and access has been heightened by the rapid transition to a managed-care-dominated health care delivery system and increased use of information technologies. Over the years, the number of health care organizations handling patient data has grown significantly. The growth of integrated delivery systems has led to the development of integrated databases of personal health information. With access to this data, people are discovering new and often improved ways to deliver effective care, identify and treat those at risk for disease, conduct population-based research, assess and improve quality, detect fraud and abuse, and market their services. Not surprisingly, these uses may raise concerns about the ability to keep information private. Some people fear that there is an increased risk that information will "leak out," or that the information may be shared—even for legitimate purposes—with people who personally know the subject of the information.

Today, some people face a conflict over whether to share information with their health care providers or avoid seeking care in order to shield themselves. When people do not fully participate in their own care, they risk undiagnosed, untreated conditions. In turn, if the information collected by health care providers and health plans is not complete and accurate, it will be less reliable for research and public health initiatives. Ultimately, the public's fear and anxiety over the loss of privacy can threaten the very initiatives meant to serve them.

8

Health privacy has often been looked at as a "balancing process"—weighing the value of disclosure against the value of privacy to an individual. This approach, however, may not always serve the interests of either patients or health care providers. Rather than weighing these interests, the Health Privacy Working Group sought to *integrate* privacy protections as part of information practices. Strong privacy protections can help to build patient trust and insure that where information is shared, it is complete and reliable.

Privacy-Protective Behavior

Many people fear their personal health information will be used against them: to deny insurance, employment, and housing, or to expose them to unwanted judgments and scrutiny. After all, the information people share with their doctors is among their most sensitive. Medical records include family history, personal behaviors and habits, and even subjective information on mental state.

Best Principles for Health Privacy

Uses of health information often extend beyond patients' current knowledge and expectations, giving rise to a profound sense of anxiety, especially when the uses are inconsistent with the original purpose for which the information was gathered.

A national survey released in January 1999[1] found that one in five people believes that his or her personal health information has been used inappropriately, without their knowledge or consent. More striking, one in six Americans engages in some form of privacy-protective behavior to shield themselves from what they consider to be harmful and intrusive uses of their health information. To protect their privacy and avoid embarrassment, stigma, and discrimination, some people withhold information from their health care providers, provide inaccurate information, doctor-hop to avoid a consolidated medical record, pay out-of-pocket for care that is covered by insurance, and—in some cases—avoid care altogether.

The 1999 survey is supported by earlier research on privacy. Decades of survey research conducted by Louis Harris & Associates document a growing public concern with privacy and the protection of personal health information.[2] The 1995 Louis Harris poll found that 82% of people were concerned about their privacy, up from 64% in 1978. Nearly 60% of the public have at some point refused to give information to a business or company out of concern for privacy, up from 40% in 1990.

Benefits and Risks of Technology

The physical limits of the paper-based medical record itself have provided a modicum of protection against broad disclosure, but may also prevent providers, researchers, and others from getting information quickly and efficiently. Paper records are burdensome: different pieces of an individual's medical information can be kept in several different places, patient histories are recorded at almost every visit, notes are written by hand, and important information can be buried in a chart. Consequently, it has often been expensive and difficult to access needed information.

The increased use of new information technologies stands to offer many public health benefits. Information maintained in electronic form can be more efficiently collected, sorted, analyzed, and transmitted. As such, it can be accessed more easily for direct patient care, to coordinate care, and in emergency circumstances; it can be analyzed for population-based trends and may serve to reduce administrative costs by more easily transmitting information for the purposes of payment, referrals, and other functions.[3]

In terms of patient privacy, there are additional benefits: in many ways electronic health information may be more securely protected than paper records by limiting access, monitoring

---

[1] California HealthCare Foundation, *National Survey: Confidentiality of Medical Records* (January 1999). The survey was conducted by Princeton Survey Research Associates. Top-line results are available at http://www.chcf.org/conference/survey.cfm.

[2] Louis Harris & Associates, *Harris-Equifax Consumer Privacy Surveys* (published in 1992, 1995 and 1996). See also Louis Harris & Associates *Health Information Privacy Survey* (1993). All surveys were conducted for Equifax, Inc.

[3] See Paul Clayton, "Technical Measures for Protecting the Confidentiality of Computer-based Health Records," in *Protecting the Confidentiality of Patient Information in a Rapidly Changing Health Care System: Summary of a National Conference*, Appendix D (Health Systems Research, Inc. eds., 1998). The conference was sponsored by the Robert Wood Johnson Foundation, held January 14, 1998 in Washington, D.C.

Background and Overview

users, and stripping data of personal identifiers before it is shared with third parties. At the request of the National Library of Medicine, the National Research Council conducted a study on privacy and security of health care information. Their report, published in 1997, found that the technology to protect data is readily available and not particularly costly. Still, there are few incentives to use privacy-enhancing technologies.[4]

Ultimately, while technological security measures can greatly improve patient privacy, they do not in and of themselves resolve the larger policy questions about how data should be used, shared, and exchanged. The technology can help to protect information, but only privacy policies—articulated in laws, regulations, and organizational policies—can articulate what limits are appropriate.

National Attention to Health Privacy

National attention to medical privacy is not new: as early as 1973 there were calls for increased attention to the privacy concerns presented by the use of computers in the health care industry. In 1976, the federal Privacy Protection Study Commission, created by the Privacy Act of 1974,[5] issued a report that included a section on the confidentiality of health information, with particular attention to insurance companies.[6] The commission noted that health care providers were losing control of patient records due to increasing population mobility, changes in the medical profession, and increasing demand for access to medical records by third parties. The commission's recommendations sparked a congressional effort to enact a medical privacy bill, but the effort failed.[7]

10

Since then, there have been a number of reports devoted to the promise of, and the challenges presented by, electronic health data.[8] Professional associations such as the American Medical Association, the American Psychiatric Association, the National Association of

---

[4] National Research Council, *For the Record: Protecting Electronic Health Information* (Washington DC: National Academy Press, 1997).

[5] Privacy Act of 1974, 5 U.S.C. § 552a (1988).

[6] Privacy Protection Study Commission, *Personal Privacy in an Information Society* (Washington DC: 1977).

[7] Also of note is the Supreme Court's decision in *Whalen v. Roe*, in which the Court addressed the privacy issues posed by a New York state law that required doctors and pharmacists to report to a state agency the names of patients who were prescribed controlled drugs. Although the Court ruled that the state law and computerized patient database did not violate patient privacy, it did so only after finding that the law contained extensive confidentiality and security safeguards to protect against unauthorized use and disclosure of sensitive health information. The Court also acknowledged that the Constitutional privacy "right to be let alone" includes "the individual interest in avoiding disclosure of personal matters," noting they were "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized databanks or other massive government files." Whalen v. Roe, 429 U.S. 589 (1977)

Best Principles for Health Privacy

[8] Of particular note are: Richard S. Dick and Elaine B. Steen, Committee on Regional Health Data Networks, Division on Health Care Services, Institute of Medicine, *The Computer-Based Patient Record: An Essential Technology for Health Care* (Washington DC: National Academy Press, 1991); Office of Technology Assessment, U.S. Congress, *Protecting Privacy in Computerized Medical Information*, OTA-TCT-576 (Washington, DC: U.S. Government Printing Office, September 1993); Molla S. Donaldson and Kathleen N.

Social Workers, and the American Hospital Association have all adopted policies on protecting patient privacy. Other health care entities are moving forward to evaluate the need for new policies and security safeguards that address patient confidentiality, with particular attention to health information maintained in electronic format.

Nevertheless, state and federal laws have not kept pace with new health care delivery systems and new technology. Federal laws that apply in select circumstances include:

- Drug and Alcohol Abuse Regulations, which provide significant protections for people who receive drug and alcohol treatment at federally funded clinics;[9]
- Privacy Act of 1974, which provides protection for personal information collected and held by the government.[10]

The 1996 Health Insurance Portability and Accountability Act (HIPAA) includes a provision mandating that either Congress or the Secretary of Health and Human Services (HHS) establish an enforceable privacy regime to protect personally identifiable health information.[11] In HIPAA, Congress set itself a time limit of August 1999 for enacting a health privacy law. If Congress fails to act by that time, the secretary is required to promulgate health privacy regulations by February 2000.

To provide some guidance for legislation, HIPAA required the secretary to submit to Congress her blueprint for health privacy legislation. In September 1997, Secretary Shalala issued a set of recommendations to Congress to "enact national standards that provide fundamental privacy rights for patients and define responsibilities for those who serve them."[12] In her report, Secretary Shalala concluded that "without safeguards to assure that obtaining

---

Medicine, *Health Data in the Information Age* (Washington DC: National Academy Press, 1994); and Committee on Improving the Patient Record, Division of Health Care Services, National Research Council, *For the Record: Protecting Electronic Health Information* (Washington DC: National Academy Press, 1997).

[9] 42 U.S.C. Sec 290dd-2 (1988). Federal law does provide substantial privacy protection for people who receive drug and alcohol treatment at federally-funded clinics. The law's regulations apply strict confidentiality rules to oral and written communications of patient records, including "the identity, diagnosis, prognosis, or treatment of any patient."

[10] 5 U.S.C. 552a. The Act prohibits federal agencies from disclosing identifiable information without an individual's "prior written consent," except if the disclosure is "consistent with" the purposes for which the information was first collected. The Act also gives people the right to see, copy, and correct their records. The Privacy Act applies to identifiable health information maintained by the federal government, including records collected for Medicaid and Medicare recipients, and records of patients in federally funded hospitals. In addition, the Department of Veterans Affairs is bound by confidentiality rules covering treatment of drug and alcohol abuse, HIV, and sickle-cell anemia.

[11] Health Insurance Portability and Accountability Act of 1996, P.L. 104-191. Also known as Kassebaum- Kennedy.

[12] Secretary of Health and Human Services, *Confidentiality of Individually-Identifiable Health Information* (September 11, 1997). Recommendations submitted to the Committee on Labor and Human Resources and the Committee on Finance of the Senate; and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives pursuant to Section 264 of the Health Insurance Portability and Accountability Act of 1996. (Hereinafter "Shalala Report")

Background and Overview

health care will not endanger our privacy, public distrust could turn the clock back on progress in our entire health care system."[13]

Formation of the Health Privacy Working Group

Either through legislation, government regulation, or self-regulation, there will be significant developments with regard to health privacy in the next few years. Such developments will have a profound impact on many aspects of health care and health-related endeavors. While there is a growing body of information that speaks to patient confidentiality, this body of work remains somewhat fragmented—there is no consensus document that reflects "best principles" for health privacy agreed upon by a broad cross-section of the health care and consumer communities.

To meet this need, in June 1998 the Health Privacy Project convened the Health Privacy Working Group with the mission of achieving common ground on "best principles" for health privacy and identifying a range of options for putting those principles into practice.

The Working Group is comprised of diverse stakeholders in the health care and consumer communities. Members of the Working Group include: disability and mental health advocates; health plans; providers; employers; standards and accreditation organizations; and experts in public heath, medical ethics, information systems, and health policy. (See list of members on inside front cover and biographies in Appendix B.)

12

"Best Principles" for Health Privacy

The Working Group developed 11 principles. The intention is for the principles to be read—and implemented—as a whole. In many instances, the Working Group drew on the work of other organizations and commissions and the report credits those bodies where applicable.

The principles represent significant compromises between Working Group members. They should be seen as the workable common ground among diverse interest groups. As such, the principles reflect protections that should be considered when implementing comprehensive patient privacy policies and practices. There are a number of instances where the report flags areas for further consideration on the part of individual entities. The report also reflects the areas where Working Group members expressed a need for either a range of options or where consensus was not reached.

At every point, the Working Group sought to set appropriate limits on the use and disclosure of personally identifiable health information, while maintaining access in ways that can enhance health care. Again, the Working Group approached the issue of health privacy with an eye toward integrating privacy protections so that appropriate and necessary uses of health information could be assured, without compromising patient trust in the health care system.

Best Principles for Health Privacy

Finally, the principles were written with an eye toward multiple constituencies, such as health care organizations, policy makers,

[13] Shalala report, pp 1-2.

consumer and disability advocates, and patients. Given the approaching HIPAA deadline for legislation or regulations, the Working Group was especially sensitive that the positions taken in this document might be translated into a legislative context. It should be understood that the principles do not necessarily represent the legislative or policy agenda of individual members of the Working Group, or the organizations/constituencies that they represent. In the course of developing the principles, there were instances in which members agreed on a particular "best practice," but did not think that the practice should be mandated by law.

Scope of Principles

In order to make the most significant contribution to the on-going national dialogue on health privacy, the Working Group chose to focus on information gathered in the context of providing patient care. The report specifically addresses information gathered and used in the treatment and health insurance context.

Members recognized that there are many more instances in which health information is collected and exchanged and the need for privacy protections in those contexts is no less urgent. A mailing list or a grocery store purchase, for example, could reveal a person's medical condition. Even more information is gathered in surveys and on-line discussion groups. The principles might be applied to information gathered in these and other contexts, but members did not intend for the principles to be used in those contexts without further analysis.

The principles are also written to establish a broad framework for the use and disclosure of health information. However, a number of areas fell outside the scope of the Working Group's focus, including:

13

- special considerations about the needs of minors;
- information that locates an individual in a particular health care organization (sometimes referred to as "directory information");
- the development and use of master patient indices to locate information on individuals;
- information provided to spouses, dependents and other next of kin;
- public health reporting; and
- fraud and abuse investigations.

Finally, this report does not address one of the issues that has proven quite difficult in the political arena: the appropriate relationship between state and federal privacy laws. The principles outlined in this report should go a long way towards helping health care entities and organizations to establish a framework to protect the confidentiality of personally identifiable health information. In that light, the Working Group has outlined a set of "best principles" to be implemented along with the requirements of state and federal law.

Background and Overview

The Working Group recognizes, however, that state and federal laws are critical to bolstering and solidifying protections for personally identifiable health information. Where state and federal laws are weak, it may impair the ability of health care organizations to effectively protect health information, thereby making patients vulnerable to the misuse of the information. Current state laws vary widely in terms of the protections given to health information. The practical impact of the existing patchwork of inconsistent—and often inadequate—state law is that a health care organization may share information across state lines, but cannot trust that the information will receive adequate protections in the receiving state.

National health care delivery and payment entities are pressed to establish a more consistent privacy approach. At the same time, many consumer and disability rights groups want to insure not only that there are baseline protections across state lines, but also that heightened protections may be put into place where needed.

The Working Group did not agree on whether any federal health privacy law—if enacted—should preempt states from passing stronger laws in the future. As Congress moves to meet the HIPAA deadline, this issue will need to be resolved in the political arena.

The Working Group's aim is to recommend and promote these best principles so that—in the absence of a state or federal law—they can be translated into "best practices" to foster trust and confidence in our nation's health care system.

Best Principles for Health Privacy

BEST PRINCIPLES FOR HEALTH PRIVACY

Principle #1

Non-Identifiable Information

Principle #1

FOR ALL USES AND DISCLOSURES OF HEALTH INFORMATION, HEALTH CARE ORGANIZATIONS SHOULD REMOVE PERSONAL IDENTIFIERS TO THE FULLEST EXTENT POSSIBLE, CONSISTENT WITH MAINTAINING THE USEFULNESS OF THE INFORMATION.

This first—and overarching—principle is intended to create incentives to use information that does not identify individuals. Generally, the use and disclosure of information that does not identify individuals is not considered to compromise patient confidentiality. As such, users of non-identifiable health information should not be held to the same authorization requirements, standards or safeguards as users of information that identifies individual patients.

The full benefits of this principle will likely be realized primarily with electronic and automated records. In a paper-based environment, it is much more difficult and costly to remove, mask, or encrypt personal identifiers. Paper-based records will therefore more often remain personally identifiable.

Health Information Exists on a Continuum of Identifiability

15

Personally identifiable health information is indispensable for many activities, including the direct provision of patient care. There are many situations, however, when personal identifiers are not necessary for the success of the project or activity. Where health information does not identify individuals, concerns about privacy are greatly reduced.

Technology presents new opportunities to allow for greater access to health information—without compromising patient confidentiality—by removing, encrypting, or masking information that identifies individuals.

It is not, however, practically possible to ensure that all information is anonymous in all circumstances. Health information exists on a continuum, ranging from information that is fully anonymous to information that directly identifies an individual. Depending on the context, the same information elements may either be anonymous or may identify individuals.

The following scenarios highlight the complexity involved in making a determination about whether information is truly anonymous. At first glance, large data sets that do not contain names, social security numbers, and home addresses provide a high level of anonymity for the individual data subjects. When linked with other data, however, a person may be able to identify individuals. Conversely, in a small data set, an otherwise innocuous identifier

Principle #1

Non-Identifiable Information

(such as place of birth) may identify an individual to people within an organization or community.[14]

Recommendations

In the context of providing patient care, personal identifiers will likely be necessary. Also, the ability to link de-identified medical information back to individuals is extremely important in some circumstances. However, there are many instances where personal identifiers can be removed. Organizations should have some flexibility and discretion in determining which individual identifiers are necessary for specific projects, and the extent to which they are able to remove individual identifiers.

At the same time, laws, regulations, and organizational policies should create strong incentives to remove personal identifiers wherever possible. Perhaps the strongest incentive to remove personal identifiers is that where organizations choose to use and disclose non-identifiable health information, they should not be subject to any of the requirements that apply to personally identifiable health information. With regard to non-identifiable health information that is encrypted or linkable to personal identifiers, the information is considered non-identifiable only if the user does not have the capacity to re-link the information. Once re-linked, the information is once again considered personally identifiable.

Data users will have to weigh many considerations in determining the possibility and practicality of using privacy-enhancing technologies, such as encryption. It may or may not be appropriate to anonymize health information. Moreover, even where it is possible to use anonymous information, it may be cost-prohibitive or, in the case of paper records, time consuming as well.

16

In many situations, it is likely that the data user may not be able to guarantee that the information is truly anonymous, i.e. that there is no possibility of identifying the individual. Health care organizations will have to make a determination about the level of risk to patient confidentiality and the risk to the project in removing identifiers. Where information is being made available to the general public, for example, the organization should take additional precautions in determining whether information is anonymous. Conversely, within the health care setting, a health care organization may want to preserve the ability to link back and re-identify information, as may be the case with some research projects.

Overall:

- Patient consent is not necessary for the use or disclosure of non-identifiable health information.
- Health information should be made as non-identifiable as possible at the earliest opportunity as consistent with the purpose for which the information will be used.
- Health care organizations should make a determination about the need for personally identifiable health information in advance of the use or disclosure of health information.

---

[14] Latanya Sweeney, "Weaving Technology and Policy Together to Maintain Confidentiality," 25 *Journal of Law, Medicine, & Ethics* 98 (1997).

Principle #2

Privacy protections should follow the data.

Principle #2

Follow the Data

Health information will be used and shared for a variety of purposes. Data holders have an ethical responsibility to maintain public trust by treating health information in a confidential manner and should be held accountable for the ways in which they use, maintain, and disclose personally identifiable health information. Health information that identifies individuals should be subject to consistent requirements, regardless of the entity holding the data.

Recipients of health information should be bound by the protections and limitations attached to the data at the initial point of collection by existing or subsequent authorizations. In effect, the protections attached to the data at its source flow with it unless there is another authorization with varying protections. Responsibility for adhering to these obligations is based on a chain-of-trust model, which requires that agents, contractors, and receiving entities without their own authorization "step into the shoes" of the disclosing entities.

In practice, this principle requires that:

- Where personally identifiable health information is disclosed, the disclosing entity should condition disclosure, or write it into the disclosure agreement, that personally identifiable health information will only be used for the purposes identified and will not be further disclosed either without patient consent or other limitations by which the disclosing entity is bound.

- Recipients of health information may not re-disclose health information in personally identifiable form without specific, voluntary patient authorization for purposes outside existing authorizations or enumerated exceptions. Recipients should not use or disclose such information unless expressly permitted by an existing authorization.

This principle will need to be implemented closely with the principle that addresses authorization requirements (Principle #6). Consider the following scenario: a health plan secures a patient's authorization for the use and disclosure of health information for the purposes of treatment, payment, and business necessity. A member of the health plan may then visit a hospital. The hospital may request information from other providers, and from the health plan and may create new health information. The hospital may also have need to use and disclose the patient's information for other purposes unrelated to the health plan's needs, such as for their own accreditation and peer review activities. Those uses should not be considered "independent" because they fall under the kinds of activities the patient authorized initially.

Conversely, any recipient of health information that is not acting within the bounds of an existing authorization will have to secure a separate, independent authorization.

Principle #3

Right of Access

Principle #3

AN INDIVIDUAL SHOULD HAVE THE RIGHT TO ACCESS HIS OR HER OWN HEALTH INFORMATION AND THE RIGHT TO SUPPLEMENT SUCH INFORMATION.

Individuals should have the right to access and supplement their own health information so that they can make informed health care decisions and correct errors where appropriate. Access to audit trails and other records of disclosure can also help people understand how their health information is used and who has had access to their health information and may assist with remedying inappropriate disclosures.

Patient Access to Personally Identifiable Health Information

More than half the states currently provide people with the right to access and copy their medical records. The Health Privacy Working Group believes that patients should have access to their own medical information when it identifies them individually. Specifically:

- Individuals should have the right to see and copy their own medical records, including an accounting of disclosures, when such accounting is maintained.
- Data holders may not refuse inspection because they are owed money by the individual requesting inspection.
- Data holders may charge a reasonable fee for copying records or may provide secure on-line access to records.
- Minors who are legally able to consent to treatment should be afforded all rights to inspect and copy medical records.

18

Some health care organizations that have implemented audit trails currently allow patients to inspect the audit trail along with the medical record. Such patient access may require some time and effort on the part of a health care organization to help the patient understand an audit trail because the report will likely be coded, lengthy, and detailed. The Working Group was not in agreement about whether patients should have routine access to audit trails, but felt that allowing patients access in cases where there is a concern about improper disclosure could provide increased accountability.

Denial of Access

Access to personally identifiable health information may be denied to the subject of the information if:

- the disclosure could reasonably be expected to endanger the life or physical safety of any individual;
- the information identifies a confidential source;
- the information is compiled principally in connection with a fraud investigation or other criminal investigation and the investigation is not yet complete; or

Best Principles for Health Privacy

- the health information was created as part of an individual's participation in clinical research, the research is not yet complete, and the individual was notified in advance about their rights to access information.

Where access has been denied, the health care organization should make a determination as to whether a portion of the medical record can be made available to the patient or a designated third party.

Supplementation of Medical Records

An individual should have the right to supplement his or her own medical record. Supplementation should not be implied to mean "deletion" or "alteration" of the medical record. An individual should not be able to modify statements that document factual observations or the results of diagnostic tests or to amend the record as to type, duration, or quality of treatment the individual believes he or she should have been provided.

The focus on a right to *supplement* the record—as opposed to a right to *amend* the record—may serve to better protect patients. Where an error in the record has been made, the supplementation can serve as historical documentation. Where the patient and provider disagree, such disagreements can also be reflected in the record.

Principle #4

INDIVIDUALS SHOULD BE GIVEN NOTICE ABOUT THE USE AND DISCLOSURE OF THEIR HEALTH INFORMATION AND THEIR RIGHTS WITH REGARD TO THAT INFORMATION.

Individuals should be given easy-to-understand written or on-line notice of how their health information will be used and by whom. Only with such notice can people make informed, meaningful choices about uses and disclosures of their health information. Adequate notice can also help to build trust between providers, health care organizations, and patients in so far as it removes any element of surprise about the use and disclosure of health information.

Components of Notification

Notice should be given at the point of application for health benefits, enrollment in a health plan or health insurance company, and at an initial encounter with a provider, if outside the scope of other notifications.

Notice should include the following elements:

- *Collection of Information*: How information will be collected and the information source, such as a medical record, treatment notes, and information from third parties.
- *Uses and Disclosure of Information*: How the entity will use the information, and how, when, and for what purposes the entity will request patient authorization.
- *Patient Right to Access Health Care Information*: What

Principle #5

Safeguards

information the patient is permitted to inspect and copy and how to access such information.

- *Patient Right to Prevent or Limit Disclosure*: Where there is a legal requirement or an organization's policy permits, patients should be notified about the steps available, if any, to limit access and the consequences, if any, of refusing to authorize disclosure. Such notice should include the rights of patients who choose to pay out-of-pocket for their care. In cases where a health care organization does not permit patients to prevent or limit disclosure, the health care organization should make that known in the notice provided to patients.

- *Organization policies*: The health care organization's policy for making disclosures with and without patient authorization, such as for research purposes, to law enforcement, for treatment purposes, etc.

- Any other information relevant to the health care entity's data practices.

Ultimately, patients should know what is being done with the information collected about them.

Principle #5

20

HEALTH CARE ORGANIZATIONS SHOULD IMPLEMENT SECURITY SAFEGUARDS FOR THE STORAGE, USE, AND DISCLOSURE OF HEALTH INFORMATION.

Appropriate safeguards should be in place to protect health information from unauthorized use or disclosure. The security safeguards do not mandate specific technical controls and are intended to be appropriate for use with electronic and paper records.

Rationale

As the 1997 National Research Council (NRC) report *For the Record* concluded, technology can be used to better safeguard personal health information in electronic form than it would be protected if on a piece of paper in a file drawer. Also, technology can be used to more efficiently anonymize and de-identify personal health information.

The Health Privacy Working Group discussed the trade-off between availability of data and confidentiality. While it is possible to afford high security protections to data, such security will also make it harder to access health information for legitimate and necessary uses. For example, if all health information is afforded the highest possible security protections, the data may not be readily available in emergency circumstances.

Requirement for Security Standards in HIPAA

Best Principles for Health Privacy

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the Department of Health and Human Services (HHS) to issue security standards for "all entities, regardless of size, involved with electronic health information pertaining to an

individual." HHS has circulated proposed rules that identify a security matrix to establish minimum requirements for security.[15] The matrix includes administrative procedures, physical safeguards, technical security services, and technical mechanisms. While the regulations will only apply to payers, providers, and electronic clearinghouses, all health care organizations should look to the regulations for guidance on technical and administrative safeguards.

The proposed matrix does not mandate specific technological controls, but requires organizations to make a determination about the level of risk involved in giving or denying access and in turn define what appropriate levels of control are warranted. The proposed regulations also place a heavy emphasis on administrative safeguards that underscore an organization's greatest vulnerability—the people who have access to identifiable information.

The Working Group agreed that it would be unwise to re-open discussion about security standards that are due to be finalized soon. There is, however, a specific nexus between confidentiality and security that needs attention. Security safeguards identify the *means* by which an entity may protect the privacy of health information. The safeguards as articulated in the HHS draft regulations do not establish who should have access and for what purposes and what a patients' rights are with regard to their health information. The specific safeguards outlined below are intended to supplement the matrix being finalized by HHS.

Recommended Safeguards

21

Overall, the implementation of security safeguards will be driven by the specific confidentiality policies, authorization requirements, state and federal law, and principles organizations adopt. Some safeguards, for example, are implied from the principles outlined in this report. For instance, the principle on authorization prohibits psychotherapy notes from being shared, except as required by a health oversight agency or public health authority, or with the explicit and voluntary authorization of the individual. Health care organizations will have to implement appropriate technical safeguards to ensure compliance with this principle.

The Working Group did not discuss specific security controls at great length. There were a number of safeguards, however, that were discussed in the context of "fair information practices." They include:

- Health care organizations should endeavor to limit access to personally identifiable health information on a need-to-know basis. Employers, for example, should endeavor to restrict access to personally identifiable health information strictly to those employees who need access for payment or treatment purposes.

- In keeping with Principle #1, health care organizations should remove personal identifiers to the fullest extent

[15] For the proposed rules and comments, see the administrative simplification website of the United States Department of Health and Human Services at http://aspe.os.dhhs.gov/admnsimp.

Principle #6

Authorization

possible and practical, consistent with maintaining the usefulness of the information.

- All disclosures of personally identifiable health information should be limited to the information or portion of the medical record necessary to fulfill the purpose of the disclosure.
- Health care organizations should maintain a record of disclosures of information that identifies an individual.
- Personally identifiable health information should be used within an organization only when such information is necessary to carry out the purpose of the activity, for purposes reasonably related to the purposes for which the information was collected, and for which the patient has been given notice.
- Organizations should consider whether they are able to provide patients with a greater degree of anonymity in certain circumstances through the use of opt-outs, pseudonyms, identification numbers, or tagging information for additional protections.

Tailoring Safeguards

As organizations adopt more sophisticated technologies, they should aim to build in the appropriate level of privacy protections.

22

Principle #6

PERSONALLY IDENTIFIABLE HEALTH INFORMATION SHOULD NOT BE DISCLOSED WITHOUT PATIENT AUTHORIZATION, EXCEPT IN LIMITED CIRCUMSTANCES. HEALTH CARE ORGANIZATIONS SHOULD PROVIDE PATIENTS WITH CERTAIN CHOICES ABOUT THE USE AND DISCLOSURE OF THEIR HEALTH INFORMATION.

The Working Group agreed that, as a general rule, patient authorization should be obtained prior to disclosure. At the same time, patient information needs to be shared for treatment, payment, and core business functions. The Working Group agreed that the patient need only provide authorization for these core, essential uses and disclosures once. Furthermore, a health care organization can condition the delivery of care or payment for care on receiving this Tier One authorization. All other activities outside this core group must be authorized separately by the patient and health care services should not be conditioned on receiving this Tier Two authorization. The Working Group also agreed that there are additional, limited activities—such as public health reporting and emergency circumstances—for which patient authorization should not be required.

Rationale

Today, most health care organizations require some form of patient authorization for the use and disclosure of health information. An authorization may be requested at the point of enrollment in a health plan, and/or when a patient sees a provider for the first time.

Typically authorizations are worded broadly enough to encompass many different kinds of activities. Additional authorizations may be collected for specific activities such as releasing a record to a new provider, for participation in a research study, or for obtaining life insurance. Some states also require additional and specific authorizations for specific conditions such as HIV/AIDS, drug and alcohol treatment, and mental health.

Patient authorization is a critical component of protecting patient privacy. Because the disclosure of health information can have significant consequences for individuals, they should have some control over the use and disclosure of personally identifiable health information.

Further, the process of obtaining patient authorization can also define an "initial moment" in which to educate patients and elicit special individual patient concerns about confidentiality. As a general rule, requiring patient authorization prior to disclosure can:

- bolster patient trust in providers and health care organizations by acknowledging the patient's role in health care decisions;
- serve as recognition that notice was given and the patient was aware of the risks and benefits of disclosure; and
- define an "initial moment" in which patients can raise questions about privacy concerns and learn more about options available to them.

23

At the same time, health information must be shared for a variety of activities in order to provide care, pay for care, and ensure the effective operation of the health care system. For some organizations, and especially networked delivery systems, it would be administratively burdensome and costly to obtain patient authorization prior to each use or disclosure.

The Working Group, therefore, agreed upon an authorization structure that allows for a health care organization to consolidate certain essential—or core—activities in a single, one-time authorization. Moreover, because these are critical—but limited—activities, the health care organization may condition the delivery of care or payment for care on receiving an authorization for these core treatment, payment, and business purposes. All other activities outside this core group should be authorized separately by the patient and he or she can refuse authorization without suffering any adverse consequences. The Working Group also agreed that there are additional, limited activities for which patient authorization should not be required. They are outlined in this report.

The basic framework here is a two-tiered authorization structure. Core activities are placed in Tier One, where the health care organization is given more discretion to make decisions about disclosure. In these circumstances, patient authorization functions as evidence that individuals have been given notice about information practices. For those activities that are not core, and therefore not

Principle #6

Authorization

itemized in Tier One, patients are given the ability to control disclosures of their health information without the delivery of care or payment for care conditioned on the receipt of the authorization. In other words, for this Tier Two set of activities, signing an authorization is voluntary and optional.

It should be noted that in arriving at this structure, the Working Group considered other authorization models. The Secretary of Health and Human Services, for example, recommended a model in which the use and disclosure of identifiable information for treatment and payment would be exceptions to the authorization requirements. In effect, the patient would implicitly authorize the use and disclosure of information for select activities by virtue of enrolling in a health plan or presenting for care. The underlying assumption of the secretary's recommendations is that most patients do not read authorization forms and do not have a meaningful opportunity to object to a core set of disclosures. The secretary's intent was to lend greater value to the authorization process by ensuring that where an authorization is presented, it is truly voluntary and uncoerced.

However, the Working Group agreed that there is a value in requiring patient authorization even for the core activities where patient authorization is, in practice, a signed acknowledgment that the authorization has been read. Again, the authorization requirement can define a moment in which patients can assess their concerns about confidentiality and take actions—such as paying out-of-pocket for care or seeking care from a particular entity—to preserve the confidentiality of their health information.

24

The framework outlined below provides for a workable middle ground: it requires patient authorization, but allows health care organizations to deny treatment or payment if authorization is refused for the critical, Tier One activities.

Obtaining Patient Authorization

The organization disclosing health information is responsible for ensuring that the appropriate authorization is obtained prior to disclosure. The authorization for core Tier One activities may be obtained at the point of enrollment or at the time of treatment, after adequate notice of information practices has been given. The authorization should be considered valid until a patient leaves a plan or insurer, or changes providers. The authorization may be revoked at any time, with certain limitations.

Authorization from a policy-holder should not be understood to include authorization for all individuals covered in that policy. Health care organizations should obtain an authorization from each individual who is legally able to provide authorization and is covered by the insurance policy or is seeking care.

Tier One Authorization	Tier Two Authorization	Uses and Disclosures Allowed without Patient Authorization
Health care organizations can obtain a single consolidated authorization for all Tier One activities. Furthermore, the health care organization may refuse to provide treatment or to pay for care if a patient refuses to provide authorization.	Activities not listed under Tier One should be authorized separately. A patient can refuse authorization without suffering negative consequences. This list is illustrative of the kinds of activities that health care organizations may place in this category— it is not intended to be a finite list.	There are a limited number of circumstances in which personally identifiable health information may be disclosed without patient authorization.
Treatment: The sharing of information necessary for the direct provision of care to a specific patient *Payment:* The sharing of information necessary to provide payment for health care. *Business Necessity:* Business necessity is understood to include the sharing of information necessary for the administrative and technical operation of a health care organization. **Note:** Where a patient self-pays, he or she can refuse to authorize disclosure to a payer.	All activities not covered in the Tier One authorization or in the exceptions to patient authorization. The activities listed below are illustrative and not a finite list of activities that need additional authorization. For purposes of marketing. For the disclosure of psychotherapy notes. For disclosure of personally identifiable information to an employer, except where necessary to provide or pay for care. For disclosure of personally identifiable health information outside the organization or agency. (Note: agents and contractors are not considered to be outside the agency.) For the disclosure of personally identifiable health information, if adequate notice has *not* been given at the point of the initial authorization.	*If the information does not identify an individual:* Patient authorization is not needed for the use and disclosure of information that is anonymous. *When required by law:* Health information may be used and disclosed without patient authorization when specifically required by law, such as for public health reporting. *For oversight purposes:* Health information may be used and disclosed without patient authorization for use in legally authorized fraud and abuse investigations. *If compelled by a court order:* Health information may be used and disclosed without patient authorization if required by compulsory legal process, such as a warrant or court order. *For research:* If consistent with Principle #8.

Principle #6

Authorization

Authorization Requirements for Core Activities: Tier One

The Working Group agrees that it is possible to establish a "one-time," durable authorization for those activities that are necessary and routine: namely, activities that are directly tied to treatment, payment, and business necessity.

There was considerable discussion about what constitutes a "core" activity. Members wanted to be broad enough to accommodate a rapidly changing health care system—activities not considered essential now may be in the future. At the same time, because authorization for core activities is non-negotiable from the patients' perspective, it was important to limit the range of activities to those that are truly necessary for the delivery of care and effective operation of the health care system.

Treatment

Treatment is understood to be the direct provision of care to a specific patient. In most circumstances, it is desirable for the treating physician to have access to the complete medical record. Health care providers may also share information about individual patients in the course of treatment—in consultation with another provider, in a referral to another provider, or in follow-up activities. In a managed care context, treatment is understood to include the sharing of information necessary to coordinate care between providers in a common network or integrated delivery system.

26

There was considerable discussion about the scope of "treatment"—and whether some activities that might be considered treatment may need special consideration in terms of the authorization requirements. Disease management, for example, is defined by "a systemic, population-based approach to identify persons at risk, intervene with specific programs of care, and measure clinical and other outcomes." In so far as the disease management program is addressing the health care concerns of specific individuals, it is considered "treatment," and needs to be conducted with information that identifies individuals. But disease management may also include an administrative, quality, or research component not directly associated with an individual.

Some consumer concerns about disease management programs are that they are often contracted out to third parties; may include a marketing or promotional component; or that patients may not receive adequate notice about the program.

At the same time, there are many benefits to disease management programs. Where the program is conducted to bring patient care up to "best practices," the program stands to improve outcomes and reduce costs. Moreover, because the health plan or payer may be assuming financial risk for the patient, it is in their interest to identify and manage high-risk patients.

Best Principles for Health Privacy

Disease management may be considered a Tier One activity, when it is conducted as part of a treatment regimen. The Working Group, however, is not recommending specific authorization requirements

for disease management programs given the differences in disease management programs as they are currently conducted. The Working Group does recommend that when conducting disease management programs, health care organizations should consider:

- the sensitivity of the medical condition being addressed;
- whether patients were given notice up-front about the existence of disease management programs;
- the manner in which patients are being contacted once enrolled in the program; and
- the practicality of allowing patients the ability to opt-in or opt-out of the program.

Disease management programs are still in an early stage of development, which presents particular challenges with regard to notification and authorization. A patient might be treated for a certain condition—such as high blood pressure—for many years when a new program becomes available. The result is that existing authorization forms and notification may not adequately address the new program. Some health care organizations have chosen to implement disease management programs through a provider. A physician's office may make contact with the patient or approve the contact with the patient through another medical professional. In such circumstances, specific patient consent may not be required, but the provider can help to make decisions about whether the use or disclosure is appropriate.

27

Restricting Use and Disclosure of Psychotherapy Notes

The Working Group agreed that where psychotherapy notes are separate from the medical record, they should not be shared without specific patient consent. Unlike information shared with other providers for the purposes of treatment, the psychotherapy notes are more detailed and subjective and are subject to unique rules of disclosure.[16] In addition, the notes are not ordinarily shared with the individual patient. A tension is created if the notes are shared beyond the provider when they are not made available to the patient. The notes are of primary value to the specific provider and the promise of strict confidentiality helps to ensure that the patient will feel comfortable disclosing information essential to the therapeutic relationship.

The phrase "psychotherapy notes" includes only the personal notes taken by a mental health professional. The notes do not include diagnostic and treatment information, signs and symptoms, or progress notes, which may be shared in the same manner as other clinical information.

---

[16] Jaffee v. Redmond, 116 S. Ct. 1923 (1996). In *Jaffee v. Redmond*, the Supreme Court ruled that conversations and notes between a patient and therapist are confidential, and that the traditional doctor/patient privilege required that they be protected from compelled disclosure. The Court found that "[e]ffective psychotherapy depends on an atmosphere of confidence and trust, and therefore the mere possibility of disclosure of confidential communications may impede the development of the relationship necessary for successful treatment. The privilege also serves the public interest, since the mental health of the Nation's citizenry, no less than its physical health, is a public good of transcendent importance."

Principle #6

Authorization

Segregation of the notes by health care providers will be critical in implementing and enforcing these heightened privacy protections.

Restricting Disclosure for Treatment Purposes

While there are few authorization requirements for uses related to treatment, not all information collected in a treatment context should be made available to all practitioners. Information is only available on a need-to-know basis—it must be relevant to the care of the patient at that time. Access to a history of reproductive services, for example, would likely not be relevant if a patient were admitted for a sprained ankle. Decisions about whether information is relevant will have to be made within an organization and by individual providers. In emergency circumstances, for example, it may be assumed that the provider may have the ability to access the entire medical record. In other circumstances, the health care organization or provider may consider restricting access within a treatment context.

Patients may have the ability to restrict additional disclosures related to treatment, but such considerations should be made on a case-by-case basis between the health care provider and the patient.

There will be special situations in which patients will have specific concerns about the confidentiality of their health information. A patient may have friends or relatives who are employees of the health care organization. A patient may also be reticent to access care at all. Where fears about confidentiality may be a barrier to treatment, the health care organization may want to accommodate a patient's desire to use a pseudonym when seeking care or to more tightly control access and disclosure of an individual patient's health care information.

28

Health care organizations may also want to allow people the ability to limit disclosure for disease management and other programs intended to supplement care delivered by a physician. A patient may have concerns about receiving mail or a phone call at home. Such concerns may be more frequently associated with certain services, such as family planning and mental health treatment. The health care organization may choose to accommodate such concerns.

A health care organization will have to make a judgement about their capacity to accommodate a patient's desire to shield information, but should aim to provide greater anonymity through the use of pseudonyms, encryption, or other techniques to shield the identity of an individual.

Payment

Disclosure and use for payment purposes includes the sharing of information necessary to make payments for health care services. In addition, payment is understood to include:

- Utilization review: "A process to determine which health services are medically necessary and appropriate (and therefore, which services are covered under the health benefits contract)."[17]

[17] American Accreditation HealthCare Commission/URAC, *Survey of State Health Utilization Review Laws and Regulations*, p.9 (Washington D.C: 1999).

- Precertification: "The process of obtaining certification or authorization from the health plan for routine hospital admissions (inpatient or outpatient). Often involves appropriateness review against criteria and assignment of length of stay. Failure to obtain precertification often results in a financial penalty to either the provider or the subscriber."[18]

- Justification of charges and coverage determinations including medical necessity.

As always, disclosure should be limited to the amount necessary to process the claim. Where the payer is also the employer, only information necessary to process a claim should be shared in personally identifiable form with employer's benefits personnel. (See Principle #10 on discrimination.)

Restricting Disclosure for Payment Purposes

A patient may explicitly limit disclosure of personally identifiable health information to a payer if he or she pays for care out-of-pocket. It should be emphasized that where a patient self-pays, it only limits disclosure to a payer; the information may still be used for other Tier One activities.

Business Necessity

Business necessity is understood to include the sharing of information necessary for the administrative and technical operations of a health care organization. Not every health care organization will have the same management needs. While a health care organization may contract out for these services, they are activities that are conducted using "in-house," or member, information. Business necessity may include:

29

- Auditing: Reviews of services delivered and billing to them to assure compliance with fraud and abuse statutes.

- Credentialing: "Obtaining and reviewing the documentation of professional providers. Such documentation includes licensure, certifications, insurance, evidence of malpractice insurance, malpractice history, and so forth. Generally includes both reviewing information provided by the provider and verification that the information is correct and complete. A much less frequent use of the term applies to closed panels and medical groups and refers to obtaining hospital privileges and other privileges to practice medicine."[19]

- Accreditation: A voluntary review by private-sector organizations. Accreditation is looked to as an important measurement by payers. It may also be a requirement of participation in certain payment programs, such as Medicare.

- Quality assurance: The use of patient information to evaluate care for a particular population.

[18] Peter Kongstvedt, *The Managed Health Care Handbook, Third Edition* (Maryland: Aspen Publishers, 1996) at 1000. (Hereinafter "Kongstvedt.")

[19] Kongstvedt at 991.

Principle #6

Authorization

- The creation of non-identifiable health information.

Many of these activities could be conducted with information that does not identify individual patients, but that may not always be practical, especially in a system that relies on paper medical records. Because consent for activities considered "business necessity" may be non-negotiable from the patient's perspective, the Working Group agreed that it was important to provide additional guidance to health care organizations about making a determination about the use of health information for these activities. Consideration should be given to the following questions:

- Is the activity necessary for the optimal performance of the organization?
- Is identifiable information necessary, or why is it impracticable to remove, mask, or encrypt personal identifiers? and
- Can patients withhold their consent for their identifiable information being used for any of the activities?

To the extent feasible, health care organizations should strive to educate patients about the use of their personally identifiable health information for purposes of business necessity. The organization's specific practices in this area should be clearly defined and incorporated into the notice provided to patients.

30

Restricting disclosures for business necessity

Based on the above standard, the health care organization should make a determination about whether patients have the ability to restrict disclosures. Health care organizations, however, should use information that is as non-identifiable as possible for these activities, where feasible.

Accommodating Sensitive Conditions

The Working Group determined that the two-tiered authorization structure was generally adequate. However, health care organizations may want to evaluate the need for additional authorization requirements for those conditions that have a history of stigma and discrimination.

A number of states have stringent authorization requirements for some health conditions. California, for example, requires specific patient authorization each time HIV/AIDS information is shared or disclosed, even between providers.[20] Massachusetts requires that an authorization for the disclosure of HIV/AIDS information be separate from other authorizations.[21] While the Working Group did not specifically endorse a more restrictive authorization model, certain organizations may want to consider additional models that provide heightened protections for their patient population.

The Working Group acknowledged that health care organizations should consider whether unique authorization requirements should be

[20] Cal. Health and Safety Code § 120985 (a) (Deering 1997).

[21] Mass. Ann. Laws ch.111, § 70F (West 1998).

established for highly sensitive information including information about HIV/AIDS and other sexually transmitted diseases, reproductive health, genetic information, abuse and neglect, drug and alcohol abuse, and mental health.

Additional authorization requirements may be particularly helpful in terms of allowing patients more control of the availability of information within an entity. A person with a stigmatized condition, for example, may not be willing to seek treatment if a relative or friend is an employee of the health care organization. Likewise, a public figure may need to seek care under a pseudonym.

Either by law or practice, some organizations require explicit authorization for the disclosure of certain "sensitive" information, even for treatment and payment. In these cases, a general, Tier One authorization is not adequate. In some circumstances, the authorization can be obtained from the patient. In others, the health care organization may ask the provider to authorize disclosure.

Patient concerns about confidentiality may center on the availability of personally identifiable health information to specific people: a certain provider, an employee, a payer, or the public. These additional authorization requirements could allow patients to have greater control of their health information without jeopardizing the delivery of care or business operations.

Finally, health care organizations should remain flexible in terms of what counts as a "sensitive condition." Emerging technologies, such as genetic testing, may present new confidentiality concerns. Even on an individual level, different conditions will be considered sensitive to different people. Family situation, care setting, and diagnosis can all affect how and whether individuals perceive their health information to be "sensitive." Health care organizations are encouraged to respond to individual concerns, and to revise authorization policies as necessary.

31

Authorization Requirements for Non-Core Activities: Tier Two

All activities not within Tier One fall into Tier Two which requires a separate, specific authorization from the patient. The delivery of care or payment for care cannot be conditioned on receiving this Tier Two authorization. A health care organization should receive separate authorization from each individual who is of legal age to consent to treatment.

Tier Two will include many activities. Additional and separate consent, for example, may be necessary for the following illustrative examples:

- For the disclosure of psychotherapy notes. (See earlier discussion: "Restricting Use and Disclosure of Psychotherapy Notes")
- For disclosure of personally identifiable health information to an employer, except where necessary to provide or pay for care. When information is shared with employers, it may not be used for promotion, hiring/firing, except as the

Principle #6

Authorization

medical condition affects the person's ability to carry out the job even with reasonable accommodation.

- For disclosure of personally identifiable health information outside the organization or agency. (Note: agents and contractors are not considered to be outside the organization or agency. A health care organization, for example, may hire a company to suggest steps to improve the quality of care. If in the process of executing the contract, the company reviews patient information, it would not be considered a disclosure "outside the agency.")

- For the disclosure of personally identifiable health information, if adequate notice has *not* been given at the point of the initial authorization.

The list above is not intended to be comprehensive, but is illustrative of the kinds of activities that can be expected to require additional, specific patient authorization. Each health care organization should make a determination about the kinds of activities that it believes fall into this category.

Finally, for the most part, marketing activities conducted primarily for profit, and not tied to patient care, will require additional, specific patient authorization. There are some activities, however, that financially benefit the health care organization, but are aimed primarily at enhancing patient care. A health care organization may market its own services to members or patients. Such "grey areas" should be vetted through an organization's data review process (as articulated in Principle #7). The expectation is that:

32

- The organization will consider the direct benefits to the patient in determining whether specific, voluntary authorization is needed for the activity; and

- The organization will only market its own services, unless they receive specific patient authorization. A health plan, for example, should not share patient names with a pharmaceutical company who is looking to market a new medication, unless there is specific authorization. On the other hand, a health plan may market their own clinical services to patients who can be expected to benefit from the services.

Such activities should be disclosed to the patient as part of the notice of organizational policies (see Principle #4).

Uses and Disclosures Allowed without Patient Authorization

Finally, there are a limited number of circumstances in which the requirements for patient authorization can be waived, or in which personally identifiable health information can be disclosed without authorization. For the most part, these exceptions are in areas in which there are existing mechanisms—such as legal requirements or regulations—that speak to the use of the data:

Best Principles for Health Privacy

- *When required by law*: Health information may be used and disclosed without patient authorization when specifically required by law, such as for public health reporting.

- *For oversight purposes*: Health information may be used and disclosed without patient authorization for use in legally authorized fraud and abuse investigations.

- *If compelled by a court order:* Health information may be used and disclosed without patient authorization if compelled by a court order in a civil or criminal investigation.

- *For research*: Health information may be used or disclosed without patient authorization for the purposes of research, consistent with Principle #8.

- *If the information does not identify an individual*: Patient authorization is not needed for the use and disclosure of information that is non-identifiable. (See additional principles on the use of non-identifiable information and the internal data-review committee.)

The Relationship to Notice

In some respect, authorization for Tier One activities is an acknowledgment that notice has been given. Except when the patient pays for care out-of-pocket, there is little opportunity to object to certain uses or disclosures. The Working Group intends to solidify this connection by requiring additional authorization if notice has not been given. For example, if a health care organization started conducting disease management programs for the first time and had, therefore, not provided any notification to patients they would need to obtain patient authorization for participation or provide notice to patients, about the initiation of the programs. For new patients or new enrollees, the organization could simply incorporate the program in the notification and Tier One authorization.

33

By more tightly connecting the authorization and notice requirements, the Working Group seeks to ensure a more educated patient population and to minimize uses of health information that are not known to the patient.

The Relationship to Safeguards

The tiers speak only to authorization requirements. To fully appreciate the impact of the authorization requirements, they must be implemented hand-in-hand with security safeguards (see Principle #5). While the authorization requirements will help individual patients control the disclosure of their health information, the security safeguards will place additional limits on the disclosure. Many security safeguards, for example, address patients' concerns about access within an entity, limiting the amount of information disclosed to third parties, and limits on re-disclosure.

Principle #7

Organizational Policies

Principle #7

HEALTH CARE ORGANIZATIONS SHOULD ESTABLISH POLICIES AND REVIEW PROCEDURES REGARDING THE COLLECTION, USE, AND DISCLOSURE OF HEALTH INFORMATION.

Every health care organization will use and disclose health information for different purposes. An organization's confidentiality policies and procedures should be coherent, tying together authorization requirements, notice given to patients, safeguards, and procedures for accessing personally identifiable health information. As such, health care organizations should:

- generate, review, and enforce confidentiality policies;
- implement minimum safeguards needed to make the policies operational; and
- review specific projects and procedures where there are ramifications for patient confidentiality.

Taking into consideration size, range of activities, and population base, organizations should establish a review process that oversees the above responsibilities. This may be accomplished through a specific committee designated to oversee confidentiality or through an existing committee, department, or individual (in the case of a small organization). For some areas it may also be appropriate to get input from members of the community, especially representatives of populations that would be affected by the policy.

34

Internal Review

An organization's confidentiality policies will help to set broad parameters to guide the use and disclosure of health information. For routine activities—such as patient care, billing, and quality assurance—the established policies and procedures are likely to be adequate. However, there will continue to be additional internal and external demands for health information or new projects that raise concerns about patient confidentiality.

The Working Group acknowledged that many requests for personally identifiable health information are necessary and valuable. Organizations should establish a review process that helps to insure accountability for decisions about the use and disclosure of personally identifiable health information. At a minimum, the review should:

- assess the need for information that identifies individual patients;
- weigh the benefit of the activity with the risk to patient confidentiality;
- make a recommendation on the need for patient authorization; and
- identify minimum required safeguards.

Where the health care organization has chosen to share information for a particular project, patients should have access to the decision on request. Ultimately, the internal review allows organizations a great deal of flexibility, while providing patients with an organizational mechanism to oversee information uses and disclosures. The intent here is to increase accountability for individuals and organizations that are using and disclosing personally identifiable health information.

Current Practices

This principle is in keeping with current professional recommendations and has been implemented in leading health care organizations. For instance, NCQA/JCAHO accreditation standards, to be implemented soon, require managed care organizations to designate "an internal review board to create and review confidentiality policies and to review practices regarding the collection, use, and disclosure of medical information."[22] Among the board's responsibilities are to:

- review all internal and external requests for using identifiable member data;
- determine levels of authorized user access to data; and
- establish mechanisms for adhering to specific member requests to limit access to data.

Intermountain Health Care of Utah has recently established a Data Access Committee that works specifically on issues of access to data for projects outside of the Institutional Review Board's scope. The Data Access Committee "recommends policy to IHC's Board of Trustees, and individually examines and acts upon all projects that fall into the definitional grey area between operations and research. The Data Access Committee reports directly to IHC's Board of Trustees. Its members include research scientists; experts in medical informatics; practicing clinicians; medical ethicists; a knowledgeable community member not associated with IHC or with other health care delivery or research; and senior managers from IHC's care delivery operations. As an extended quorum, all IRB chairpersons working within IHC also attend to discuss problems and recommend policy supporting IRB function throughout the IHC system. A full record of each meeting is generated and maintained." [23]

35

---

[22] Joint Commission on Accreditation of Healthcare Organizations and the National Committee for Quality Assurance, *Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment* (Washington, D.C.: November 1998). The full report is available on-line at http://www.ncqa.org/confide/tablcont.htm.

[23] *Confidentiality of Medical Information Hearing*, Senate Committee on Health, Education, Labor and Pensions, 104th Cong. (February 24, 1999) (statement of Brent James, Executive Director, Intermountain Health Care Institute for Health Care Delivery Research).

Principle #8

Research

Principle #8

HEALTH CARE ORGANIZATIONS SHOULD USE AN OBJECTIVE AND BALANCED PROCESS TO REVIEW THE USE AND DISCLOSURE OF PERSONALLY IDENTIFIABLE HEALTH INFORMATION FOR RESEARCH.

The Working Group believes that it is important to create equity, fairness, and accountability in the application of confidentiality policies to research involving the use of personally identifiable health information. Such an across-the-board approach will provide more comprehensive confidentiality safeguards, as well as bolster the public's trust and confidence in research initiatives.

Currently, research that receives federal funding, or is conducted in anticipation of FDA approval, is subject to the "Common Rule,"[24] a federal regulation that requires that any use of "identifiable private information" be overseen by an Institutional Review Board (IRB). The rule was established for the purpose of supervising research and protecting "the rights and welfare of human research subjects."[25] Under the regulations, a researcher must obtain informed consent to use personally identifiable health information, unless the IRB approves a waiver or the research falls within one of the enumerated exceptions to informed consent.

Where the research is currently subject to IRB review, the Working Group agreed that consent requirements and security safeguards should continue to be addressed by the IRB. For research not currently subject to IRB review, health care organizations should either use an existing IRB or establish an objective and balanced review process to determine the need for informed consent and appropriate safeguards.

36

In all circumstances, health care organizations should ensure balance and accountability in decisions about the use of personally identifiable health information for research. Towards that end, all research—whether federally regulated or not—should be subject to a review process and the application of certain standards.

Structure: Balanced and Objective Review

Objective and balanced review can help to ensure that researchers anonymize information when possible and serve as a check on the legitimacy of the objectives of the research. Review may also be in the interest of the disclosing entity—it can help it to determine if the project is a good use of their resources, if the risk is minimal to the subjects, and if the project is of scientific merit.

Again, existing federal regulations require that certain research be approved by an IRB. The regulations specify that the IRB include at least one member who is not "otherwise affiliated with the

---

[24] 45 CFR part 46, subpart A, known as the "Federal Common Rule." The Food and Drug Administration's equivalent regulation is 21 CFR part 50 and 21 CFR part 56.

[25] Office for Protection of Research Risks, United States National Institutes of Health, *Institutional Review Board Guidebook* (1993) at 1-1. (Hereinafter "OPPR Guidebook")

institution and who is not part of the immediate family of a person who is affiliated with the institution." While the additional four members of the IRB may be affiliated with the institution, the regulations strive to establish a degree of objectivity and balance in the review of research proposals.

As noted, some research falls outside the scope of the federal regulations. Members of the Working Group were not in agreement about the merit of requiring IRB approval for all research. Preliminary studies caution that IRBs are overextended, and the qualifications of members are varied.[26] Some members of the Working Group believed that the extension of federal regulations stands to place additional burdens on IRBs and could dilute their current work. There are also concerns that IRBs are not currently composed to have the requisite experience to judge privacy concerns in research.

Members of the Working Group agreed that an evaluation of the existing IRB system was beyond the scope of its mission. Concerns with the current system were significant enough, however, that members were open to using an alternate review process in situations where IRB approval is not currently required, if it could offer the same potential benefits of the IRB system. Merits of the IRB system, that may or may not be replicable, include:

- a common and independent set of standards;
- requirements for committee composition;
- publicly available decisions; and
- accountability and oversight.

37

Again, the Working Group agreed not to assess current requirements for IRB approval. Where IRB approval is not currently required, however, a health care organization should have the option to either: 1) obtain IRB approval or 2) use an alternate process that provides an equivalent level of review and accountability.

Standard: Need for Uniformity

Much health-related research that uses personally identifiable health information is conducted with informed consent. However, for some research, it may not be practical to obtain informed consent. In other cases, the project requires full participation—allowing people to refuse participation could bias the results. The Working Group agreed that it was important to provide a mechanism to waive informed consent requirements for some research, as is currently provided under the IRB system. However, as is the case with IRBs, a waiver of informed consent should only be granted if such a determination is made through an objective and balanced process.

---

[26] United States General Accounting Office, *Scientific Research: Continued Vigilance Critical to Protecting Human Subjects*, GAO/HEHS-96-72, (Mar. 8, 1996) and Health and Human Services Inspector General, "Institutional Review Boards: A Time for Reform," OEI-01-97-00193 (June 1998). There are also three companion reports to the HHS report, released simultaneously, entitled "IRB's: Their Role in Reviewing Approved Research," "IRB's: Promising Approaches," and "IRB's: The Emergence of Independent Boards."

Principle #8

Research

Most importantly, there should be uniformity in decisions about when, and under what circumstances, to grant a waiver of informed consent. The *confidentiality* standards articulated in the current federal regulations should serve as the standards for all research—regardless of the body reviewing the proposal. As these standards are revised, they should be incorporated into the policies of the bodies reviewing research proposals.

Regulations governing federally funded research projects require the "informed consent" of "human subjects" participating in a research activity. In evaluating whether to approve a research project that intends to use identifiable data without first obtaining the informed consent of the patient, the IRB must weigh the potential risks to the individual against the "anticipated benefits to the individual or society."[27]

In most circumstances, it is assumed that the researcher will obtain the informed consent of the research participants. The Common Rule, however, allows for exceptions to the informed consent process: some research is exempt from IRB approval, some research is subject to expedited review, and some research is subject to review by the full IRB.

Exempt research: The regulations list many kinds of research that are not subject to IRB review. Of particular note is research that only involves "the collection or study of existing data, documents, records, pathological specimens, or diagnostic specimens, if these sources are publicly available or if the information is recorded by the investigator in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects."

38

Expedited review: Under an expedited review, the research project may be approved by a single member of the committee. Types of research that may undergo expedited review are periodically updated by the Secretary of Health and Human Services. Overall, to be eligible for expedited review, the research must (1) involve no more than "minimal risk"[28] or (2) or involve only "minor changes in previously approved research during the period (of one year or less) for which approval is authorized."

In addition to these exceptions, an IRB may alter or waive the consent requirements if the IRB finds that:

> " (1) the research involves no more than minimal risk to the subjects;
> (2) the waiver or alteration will not adversely affect the rights and welfare of the subjects;
> (3) the research could not practicably be carried out without the waiver or the alteration; and
> (4) whenever appropriate, the subjects will be provided with additional pertinent information after participation."

---

[27] OPRR Guidebook at 5-8.

[28] Minimal risk is defined as "the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in daily life or during the performance of routine physical or psychological examination or tests."

The Common Rule, as written, may not provide adequate privacy protections or appropriately address research using databases and archival records.[29] Overall, the current federal regulations are written primarily with an eye toward interventional research studies, such as clinical trials. There is less guidance for research that uses information that identifies individuals, but does not *physically* involve the patient in the research. A review of existing IRB confidentiality standards is currently underway by both HHS and the National Bioethics Advisory Council (NBAC).[30]

Principle #9

Law Enforcement

The rapid advances in research require some flexibility in standards with regard to confidentiality and research. It is important, however, that there be uniformity in terms of when, and under what circumstances, informed consent requirements can be waived. Whether research is reviewed by an IRB or through an alternate review process it should be held to the same standard. As the standard is revised, pursuant to public comment, it should be applied across the board.

Principle #9

HEALTH CARE ORGANIZATIONS SHOULD NOT DISCLOSE PERSONALLY IDENTIFIABLE HEALTH INFORMATION TO LAW ENFORCEMENT OFFICIALS, ABSENT COMPULSORY LEGAL PROCESS, SUCH AS A WARRANT OR COURT ORDER.

As a general rule, federal privacy laws require that some form of compulsory legal process, based on a standard of proof, be presented in order to disclose to law enforcement officers.[31] Law enforcement access to health information should be held to similar standards.

39

However, government officials may have legally authorized access to personally identifiable health information to engage in oversight and enforcement of law. In these instances—where compulsory legal process may not be required— information obtained for oversight purposes may not be used against an individual patient in an action unrelated to the oversight nor can the information be re-disclosed, including to another law enforcement agency, except in conformance with the privacy protections that have attached to the data.

Where access has been granted, law enforcement officials should be required to implement appropriate safeguards. In addition to the

---

[29] A recent report published by the General Accounting Office concluded that "[w]hile many organizations have in place IRB review procedures, recent studies pointed to weaknesses in the IRB system, as well as the provisions of the Common Rule itself, suggest that IRB reviews do not ensure the confidentiality of medical information used in research." United States General Accounting Office, *Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections is Limited* (Washington, D.C.: 1999) at 12.

[30] Information and draft reports of the National Bioethics Commission are available on-line at http://bioethics.gov/cgi-bin/bioeth_counter.pl.

[31] See, for example, Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681; Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401; Privacy Protection Act of 1980, 42 U.S.C. § 2000aa; Cable Communications Policy Act of 1984, 47 U.S.C. § 551; Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2703 (a); and Video Privacy Protection Act of 1988, 18 U.S.C. § 2710.

Principle #10

Discrimination

safeguards required for all data-holders (see Principle #5), every effort should be made to prevent information that may identify individuals from entering a public record.

Principle #10

HEALTH PRIVACY PROTECTIONS SHOULD BE IMPLEMENTED IN SUCH A WAY AS TO ENHANCE EXISTING LAWS PROHIBITING DISCRIMINATION.

Patients are understandably concerned that some of their health information can be used in ways to discriminate against them. While this report does not take up the larger issue of discrimination, there is a relationship between privacy protections, and the enforcement of anti-discrimination laws. Privacy protections can reduce the probability that discrimination might happen. For instance, limits on an employer's access to an employee's medical information may limit the employer's opportunity to misuse the information under existing anti-discrimination laws. In this way, privacy may be the first line of defense against discrimination.

The Working Group agreed that privacy policies should be developed and implemented in such a way as to enhance already existing anti-discrimination protections guaranteed by law. At the same time, privacy protections should not be implemented in such a fashion as to effectively create new policies on related issues. Where organizations are engaged in a legally authorized activity, they should have access to patient information, subject to the specified requirements. At the same time, privacy policies should close loopholes and fill in gaps in existing laws, consistent with the overall anti-discrimination policies already fashioned.

40

Currently, there are state and federal laws that prohibit discrimination on the basis of personally identifiable health information in areas such as employment and insurance underwriting. Also, a number of states have laws prohibiting genetic discrimination. In these areas, appropriate limits on the use of identifiable data may serve to enhance these anti-discrimination laws.

Employer Use of Health Information

Employers use health information for a variety of purposes including employee assistance programs, worker's compensation, on-site delivery of care, and for management of health care benefits.[32] An

[32] Employer use of medical information was taken up in a 1995 court case. In *Doe v. SEPTA*, a federal court found that an employee's privacy interest in shielding his personal health information from his self-insured employers was less compelling than the employer's interest in overseeing its health care plan. A Rite-Aid drug store in Pennsylvania provided to the *Southeastern Pennsylvania Transportation Authority (SEPTA)* information about the prescription drugs being taken by SEPTA's employees. The stated purpose of the disclosure was to allow the state to monitor the costs of its prescription drug program. However, in disclosing to SEPTA authorities that one of its employees was receiving AZT, Rite-Aid in effect disclosed the employee's HIV status. Prior to the disclosure, Doe's employers had assured him that although they were self-insured, no information regarding his prescription drugs or HIV status would be disclosed outside of the Medical Department. The court found no privacy violation stemming from this disclosure since Doe could not prove actual damages and the employer was deemed to have a legitimate interest in knowing the details of how its employees used the health plan. *Doe v. Southeastern Pennsylvania Transportation Authority (SEPTA)*, 72 F.3d 1133 (1995).

employer, for example, may be required to provide "reasonable accommodation" for a disability under the Americans with Disabilities Act.[33] In providing the accommodation the employer may obtain sensitive employee health information. It is not the intent of the Working Group to interfere with the operation of these duties.

There is concern, however, that employer access to health information for these purposes opens the door for employers to use the information for other purposes. Limitations on employer access to, and use of, employee medical data should: 1) not interfere with provisions of the Americans with Disabilities Act (ADA) requiring employers to make reasonable accommodations for people with disabilities; and 2) should close the loop that currently allows employers access to, and use of, employee data in ways not required under the ADA. In many ways, privacy is the first line of defense against discrimination, shielding from employers sensitive employee data that is unrelated to their ability to perform a particular job.

Principle #11

STRONG AND EFFECTIVE REMEDIES FOR VIOLATIONS OF PRIVACY PROTECTIONS SHOULD BE ESTABLISHED.

To be truly effective, health privacy policies must be buttressed by a set of comprehensive and strong remedies for violation of the policies. It is important that remedies be available for internal and external violations of confidentiality. Unauthorized access within an entity, for example, can be as harmful as disclosure to an outside entity.

41

Health care organizations should establish appropriate employee training, sanctions, and disciplinary measures for employees and contractors who violate confidentiality policies. Such measures may take into consideration intentional and unintentional actions.

[33] For more information on employer responsibilities under the ADA, see Chai Feldblum, "Medical Examinations and Inquiries Under the Americans with Disabilities Act: A View from the Inside," 64 *Temple Law Review* 521 (1991).

Definitions

Definitions

Anonymous health information: Information that contains details about a person's medical condition or treatment but the identity of the person cannot be identified.[34]

Disclosure: Sharing of patient information outside an entity. Agents and contractors are considered within an entity (see use).

Health care organizations: A health care organization is any entity that collects, uses, or has access to patient information. The term includes, but is not limited to, health care providers, health plans, public health authorities, employers, life insurers, schools and universities, and health care clearinghouses.

Health information: The term health information means any information, whether oral or recorded in any form or medium, that—(A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.[35]

Non-identifiable health information: Health information from which personal identifiers have been removed, masked, encrypted or otherwise concealed, such that the information can not reasonably be expected to identify individual patients.

42

Personally identifiable health information: Health information that contains information such that an individual person can be identified as the subject of that information.

Use: Access or sharing of information within an entity, including to an agent or contractor of an entity.

---

[34] Adapted from Latanya Sweeney, "Weaving Technology and Policy Together to Maintain Confidentiality," 25 *Journal of Law, Medicine, & Ethics* 98 (1997).

[35] Health Insurance Portability and Accountability Act of 1996, P.L. 104-191. Also known as Kassebaum- Kennedy.

APPENDIX A: RESOURCES

Randolph C. Barrows, Jr. and Paul D. Clayton, "Privacy, Confidentiality, and Electronic Medical Records," 3 *Journal of the American Medical Informatics Association* 139 (1996).

Paul Clayton, "Technical Measures for Protecting the Confidentiality of Computer-based Health Records," *Protecting the Confidentiality of Patient Information in a Rapidly Changing Health Care System: Summary of a National Conference*, Appendix D (Health Systems Research, Inc. eds., 1998). The conference was sponsored by the Robert Wood Johnson Foundation, held January 14, 1998 in Washington, D.C.

Janlori Goldman and Deirdre Mulligan, Foundation for Health Care Quality, *Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality* (Washington: 1996).

Janlori Goldman and Zoe Hudson, *Promoting Health/Protecting Privacy: A Primer* (California: 1999). Prepared for the California HealthCare Foundation and Consumers Union.

Janlori Goldman, "Protecting Privacy to Improve Health Care," 17 *Health Affairs* 47 (November-December 1998).

Janlori Goldman, "Privacy and Health Information: A Legal Framework," *Protecting the Confidentiality of Patient Information in a Rapidly Changing Health Care System: Summary of a National Conference*, Appendix E (Health Systems Research, Inc. eds., 1998). The conference was sponsored by the Robert Wood Johnson Foundation, held January 14, 1998 in Washington, D.C.

Lawrence Gostin, "Health Information Privacy," 80 *Cornell Law Review* 451 (1995).

Lawrence Gostin et al, *Legislative Survey of State Confidentiality Laws, with Specific Emphasis on HIV and Immunization, Final Report Presented to: The U.S. Centers for Disease Control and Prevention; The Council of State and Territorial Epidemiologists; The Task Force for Child Survival and Development Carter Presidential Center* (1997). The report is available at (http://www.epic.org/privacy/medical/cdc_survey.html)

Lawrence Gostin et al, "The Public Health Information Infrastructure: A National Review of the Law on Health Information Privacy," *Journal of the American Medical Association* 391 (June 26, 1996).

Institute of Medicine, *The Computer-Based Patient Record: An Essential Technology for Health Care* (Washington DC: National Academy Press, 1997). The report is available at http://www.nap.edu/readingroom/.

Institute of Medicine, Committee on Regional Health Data Networks, *Health Data in the Information Age* (Washington DC: National Academy Press, 1994). The report is available at http://www.nap.edu/readingroom/.

Appendix A

Resources

International Society for Pharmacoepidemiology, *Data Privacy, Medical Record Confidentiality, and Research in the Interest of Public Health* (Washington DC: September 1997). The report can also be found at http://www.pharmacoepi.org.

Shannah Koss, "White Paper - Health Insurance Portability and Accountability Act: Security Standards; Implications for the Healthcare Industry," IBM White Paper (1998). The paper is available at http://www.solutions.ibm.com/healthcare/solution/whitep1.html.

Bernard Lo, "Confidentiality of Patient Information in a Changing Health Care System" in *Protecting the Confidentiality of Patient Information in a Rapidly Changing Health Care System: Summary of a National Conference*, Appendix F (Health Systems Research, Inc. eds., 1998). The conference was sponsored by the Robert Wood Johnson Foundation, held January 14, 1998 in Washington, D.C.

Bernard Lo, *Resolving Ethical Dilemmas: A Guide for Clinicians* (Baltimore, Maryland: Williams and Wilkins, 1995).

William Lowrance, U.S. Department of Health and Human Services, *Privacy and Health Research: A Report to the U.S. Secretary of Health and Human Services* (May 1997). The report is available at http://aspe.os.dhhs.gov/datacncl/PHR.htm.

National Committee for Quality Assurance and the Joint Commission on Accreditation of Healthcare Organizations, *Protecting Personal Health Information: A Framework for Meeting the Challenges in a Managed Care Environment* (Washington DC: 1998). The report is available at http://www.ncqa.org/confide/tablcont.htm.

National Committee on Vital and Health Statistics, *Health Privacy and Confidentiality Recommendations* (Washington DC: June 25, 1997). Full text is available at http://aspe.os.dhhs.gov/ncvhs/privrecs.htm.

National Research Council, *For the Record: Protecting Electronic Health Information* (Washington DC: National Academy Press, 1997). Full text is available at http://www.nap.edu/readingroom/.

Office of Technology Assessment, United States Congress, *Protecting Privacy in Computerized Medical Information* (September 1993). The report is available at http://www.wws.princeton.edu/~ota/ns20/alpha_f.html.

The President's Advisory Commission on Consumer Protection and Quality in the Health Care Industry, *Quality First: Better Health Care for All Americans* (1998). See Appendix A: Consumer Bill of Rights and Responsibilities, pp. A57-A60 for "Confidentiality of Health Information." To order, call 800-732-8200; ISBN 0-16-049533-4.

William Roach and the Aspen Health Law and Compliance Center, *Medical Records and the Law.* (Gaithersburg, Maryland: Aspen

Publishers, 1998).

Latanya Sweeney, "Controlling Inference and Protecting Privacy by Constructing an Anonymous Data System" (Carnegie Mellon University: Unpublished paper, November 1998).

Latanya Sweeney, "Weaving Technology and Policy Together to Maintain Confidentiality," 25 *Journal of Law, Medicine, & Ethics* 98 (1997).

United States Department of Health and Human Services, *Confidentiality of Individually-Identifiable Health Information, Recommendations Submitted to Congress* (September 1997). Full text is available at http://aspe.os.dhhs.gov/admnsimp/pvcrec0.htm.

United States Department of Health and Human Services, *Administrative Simplification Home Page.* Includes proposed Rules and Comments, http://aspe.os.dhhs.gov/admnsimp.

United States Department of Labor, *Genetic Information and the Workplace* (January 20, 1998). The report is available at http://www.dol.gov/dol/_sec/public/media/reports/genetics.htm.

United States General Accounting Office, *Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections Limited* (GAO/HEHS-99-55, February 1999).

APPENDIX B: MEMBER BIOGRAPHIES

Paul Clayton

Paul D. Clayton, a native of Salt Lake City, Utah, received his Ph.D. in physics from the University of Arizona in 1973. He then developed and implemented information systems in cardiology, radiology and surgery at LDS Hospital and the University of Utah. He joined Columbia in 1987 as director of the Center for Medical Informatics and professor of medical informatics. He became chairman of the newly created Department of Medical Informatics in 1994. When Dr. Clayton joined Columbia, he led efforts to build an integrated information system for the medical center, an effort supported by an Integrated Advanced Information Management System grant from the National Library of Medicine. He was also active in creating an advanced clinical information system with decision-making capability now widely used at CPMC. Dr. Clayton is president of the American Medical Informatics Association and an elected fellow of the American College of Medical Informatics and the Institute of Medicine. Dr. Clayton chaired a National Research Council committee addressing issues of confidentiality of health records on the national information infrastructure.

Jeff Crowley

Jeff Crowley is the deputy executive director for programs of the National Association of People with AIDS (NAPWA). Mr. Crowley oversees NAPWA's education department and the community development and training department. He is a co-chair of the Health Task Force of the Consortium for Citizens with Disabilities and has convened the Coalition for Emergency Action on Medicaid Funding. Mr. Crowley is also a member of the National Academy for State Health Policy's Working Group on Medicaid Managed Care for People with AIDS. He received his bachelor of arts from Kalamazoo College in Michigan where he majored in chemistry and earned a master's in public health from Johns Hopkins University.

John Glaser

John Glaser is vice-president and chief information officer, Partners HealthCare System, Inc., an integrated delivery system founded by the Brigham and Women's Hospital and Massachusetts General Hospital. Previously, he was vice-president, information systems at Brigham and Women's Hospital.

He was founding chairman, College of Healthcare Information Management Executives (CHIME) and past-president, Healthcare Information and Management Systems Society (HIMSS). He is the 1994 recipient of the John Gall award for Healthcare CIO of the year.

Prior to Brigham and Women's Hospital, Dr. Glaser managed the Healthcare Information Systems consulting practice at Arthur D. Little. He holds a Ph.D. in Healthcare Information Systems from the University of Minnesota.

Nan Hunter
Nan D. Hunter is a professor of law at Brooklyn Law School. In the spring of 1998, she was a visiting professor of law at Harvard Law School. In 1986, prior to entering teaching, she founded and became the first director of the ACLU AIDS Project. From 1993 to 1996, she was deputy general counsel at the U.S. Department of Health and Human Services. In 1997, she was appointed to the President's Advisory Commission on Consumer Protection and Quality in the Health Care Industry. She is a Fellow of the New York Academy of Medicine. She is the author of numerous articles in the area of constitutional law, civil rights, and health law.

Shannah Koss
Shannah Koss is the health care security and government programs executive at IBM Corporation. She is the marketing manager for the government health-care segment and responsible for positioning IBM's health-care IT capabilities in response to changes in the legal requirements for the health-care market. Ms. Koss is currently leading the establishment of IBM's Healthcare Security Practice. Prior to joining IBM, Ms. Koss was the manager for the Federal Office of Management and Budget overseeing health care programs and federal health care information requirements. She was the co-chair of the Information Systems Working Group in the Clinton Administration Health Care Task Force. She has a bachelor's degree from the University of Chicago and a master's from the John F. Kennedy School of Government at Harvard University.

Chris Koyanagi
Chris Koyanagi is policy director for the Judge David L. Bazelon Center for Mental Health Law in Washington, D.C. The Bazelon Center is a legal advocacy organization concerned with the rights of children and adults with mental impairments. Chris is responsible for the legislative and policy advocacy agenda of the Bazelon Center. The Center's priorities are to ensure community membership for persons with mental illness, including access to community based services and protection of individual rights to choice. Ms. Koyanagi works on policy issues with respect to financing mental health services, particularly through Medicaid, the use of advance directives for mental health care, consumer rights under public sector managed care plans, access to housing, income support, education, rehabilitation and other essential community services for adults and children with mental disorders.

Chris has nearly 30 years of Washington experience working on human services issues and in addition to her work at the Bazelon Center, serves on several mental health policy advisory committees and has authored numerous articles and other publications on mental health policy.

Bernard Lo, Chair

Bernard Lo, M.D., is professor of medicine and director of the Program in Medical Ethics at the University of California San Francisco. He directs the national coordinating office of the Initiative to Strengthen the Patient-Provider Relationship in a Changing Health Care Environment, which is funded by the Robert Wood Johnson Foundation. He chairs the End of Life Committee convened by the American College of Physicians, which will develop recommendations for clinical care near the end of life.

Dr. Lo is a member of the National Bioethics Advisory Commission, which issued a report in June 1997 on cloning of human beings. He is also a member of the Data Safety Monitoring Board for the AIDS Clinical Trials Group at the National Institute of Allergy and Infectious Diseases. He is a member of the Institute of Medicine and serves on its Board of Health Sciences Policy. He served on the White House Task Force on Health Care Reform and the National Institutes of Health advisory board on human embryo research.

Dr. Lo has written over one hundred articles in peer-reviewed medical journals, on such issues as decisions about life-sustaining interventions, decision-making for incompetent patients, physician-assisted suicide, and ethical issues regarding HIV infection. He is the author of *Resolving Ethical Dilemmas: A Guide for Clinicians*, a comprehensive analysis of ethical dilemmas in adult clinical medicine. He is also a practicing general internist and teaches clinical medicine to residents and medical students.

John T. Nielsen

John T. Nielsen is currently Senior Counsel and Director of Government Relations for Intermountain Health Care, Salt Lake City, Utah. In that capacity he is responsible for government relations and public policy in the states of Utah, Idaho, Wyoming and also in Washington, D.C. Mr. Nielsen is a frequent witness at both the state and national level with issues involving health care, health insurance and medical records privacy and confidentiality. He also serves as a member or chairs numerous state boards and task forces dealing with health care and insurance-related issues. Mr. Nielsen is also of-counsel in the Salt Lake City firm of Van Cott, Bagley, Cornwall & McCarthy. As a senior partner in that law firm, he practiced in the area of government and legislative relations, administrative and regulatory matters, and civil and criminal litigation.

Mr. Nielsen began his career in government in 1970 as an Assistant Salt Lake City Attorney. In 1973 he became legal advisor to the Salt Lake City Police Department. Mr. Nielsen joined the office of the Salt Lake County Attorney as a felony prosecutor in 1975. He was the Chief Deputy of the Justice Division of the Salt Lake County Attorney's Office from 1979 to 1985. Mr. Nielsen was appointed Utah Commissioner of Public Safety in March 1985 serving until 1989.

He is a member of the Utah State Bar, the American Bar Association, and the American Academy of Health Care Attorneys. He also chairs or serves as a member of various government councils and

commissions, and is active in civic and church affairs. Mr. Nielsen is a native of Salt Lake City. He graduated from the University of Utah with a B.S. in Business Management in 1967 and from the University of Utah College of Law with his Juris Doctorate in 1969. He is married and has four daughters.

Linda K. Shelton
Linda Shelton is assistant vice president for product development for the National Committee for Quality Assurance (NCQA). Ms. Shelton led the team that developed Accreditation '99, which for the first time integrates HEDIS and Accreditation, and is now leading NCQA's efforts to develop new accreditation products for PPOs and other organizations. She has also developed NCQA Accreditation's public reports, conducted over 35 accreditation surveys and served as faculty for NCQA conferences. She has a master's degree in health care administration from George Washington University.

Margaret Anne VanAmringe
Ms. VanAmringe is vice-president for external relations at the Joint Commission on Accreditation of Healthcare Organizations. She is responsible for developing new strategic opportunities for the Joint Commission, especially in the area of managed care. She also directs their Washington Office, which is concerned with developing new directions for the Commission in response to federal and private sector initiatives. She works on policy issues involving outcomes and other performance measurement of health care organizations, health care privacy, quality of care oversight, and health care policy.

Just prior to taking a position at the Joint Commission, Ms. VanAmringe was director, Center for Research Dissemination and liaison at the Agency for Health Care Policy and Research in the U.S. Public Health Service. As director, she established programs to communicate health services research findings, including clinical practice guideline and outcomes research information, to a wide array of professional and public audiences. At AHCPR she developed the first extramural grant program to investigate the best methods of encouraging clinicians to change their practices based on new medical evidence. Ms. VanAmringe also initiated AHCPR's first health information dissemination program to bring practical health services research information into the hands of consumers and their families.

From 1989 to mid 1990, Ms. VanAmringe was a legislative fellow in the Office of Senator George Mitchell (D-Me.) where she drafted health legislation in areas such as health services research, biomedical research and long-term care.

From 1988 to 1989, she held several positions in the Immediate Office of the Secretary, Department of Health and Human Services, including senior advisor to the chief of staff. During these times, she provided advice on the full range of social and health policy issues. Before joining the Secretary's staff, she spent eight years working in the Health Care Financing Administration where she directed their Office of Survey and Certification, the component responsible for

assuring that health care facilities reimbursed by Medicare/Medicaid meet quality of care and safety standards.

Ms. VanAmringe is on the board of Health Commons Institute, a private not-for-profit organization whose mission is to improve Health care outcome through shared decision making between clinicians and patients using computer-assisted methodologies and databases. She received her masters degree from the Johns Hopkins School of Hygiene and Public Health.

APPENDIX C: STAFF BIOGRAPHIES

Janlori Goldman

Janlori Goldman directs the Health Privacy Project at Georgetown University's Institute for Health Care Research and Policy. Ms. Goldman created the Project in December 1997. The Project is dedicated to ensuring that peoples' privacy is safeguarded in the health care environment. In 1997, Ms. Goldman was a Visiting Scholar at Georgetown University Law Center. In 1994, Ms. Goldman co-founded the Center for Democracy and Technology, a non-profit civil liberties organization committed to preserving free speech and privacy on the Internet. Ms. Goldman also worked at the Electronic Frontier Foundation in 1994. From 1986 to 1994, Ms. Goldman was the staff attorney and director of the Privacy and Technology Project of the American Civil Liberties Union (ACLU). While at the ACLU, Ms. Goldman led the effort to enact the Video Privacy Protection Act and led efforts to protect peoples' health, credit and financial information and personal information held by the government. She was the legislative director of the Minnesota affiliate of the ACLU from 1984-86.

Ms. Goldman has testified frequently before the U.S. Congress and served on numerous commissions and advisory boards. Her publications include "A Federal Right of Information Privacy," co-authored with Jerry Berman, and included as a chapter in *Computers, Ethics, and Social Values*, ed. Helen Nissenbaum, Prentice Hall, 1995; *Privacy and Health Information Systems: A Guide to Protecting Patient Confidentiality*, co-authored with Deirdre Mulligan, Foundation for Health Care Quality, 1996; "Protecting Privacy to Improve Health Care," *Health Affairs*, Nov/Dec 1998; and most recently, *Promoting Health/Protecting Privacy: A Primer*, co- authored with Zoe Hudson, California HealthCare Foundation and Consumers Union, 1999.

Zoe Hudson

Zoe Hudson is a policy analyst with the Health Privacy Project at Georgetown University's Institute for Health Care Research and Policy. The Project is dedicated to ensuring that peoples' privacy is safeguarded in the health care environment. Ms. Hudson joined the Project in March 1998 and her responsibilities include staffing the Health Privacy Working Group, and developing a comprehensive state survey of health privacy laws. Ms. Hudson co-authored with Janlori Goldman *Promoting Health/Protecting Privacy: A Primer* for the California HealthCare Foundation and Consumers Union. In addition, Ms. Hudson has written testimony for the U.S. Congress. Before coming to the Health Privacy Project, Ms. Hudson was the program and policy director for Parents, Families and Friends of Lesbians and Gays (PFLAG), a national, grassroots organization. She received her bachelor of arts from Grinnell College in Iowa.

Ms. FELDBLUM. Was an effort by people from a whole range—consumers, industry, providers, researchers—to come up not with a template for Federal legislation, but a set of best principles that industry would voluntarily take on, that you now in Congress could look to as a model as you are trying to make the words fit the rhetoric.

Okay, so let me tell you the few things where I think the words are really problematic, but not insurmountable and then a few I think where the policy is difficult.

One, health care operations, heard this a lot. The problem with health care operations, of course, is that it is in the compelled authorization that when I go and I sign, go for treatment, I have to sign an authorization for treatment, payment and health care operations. We in CCD didn't like the idea that you had to sign up for health care operations. We love disease management. We want to see more of it, but we want it to have the chance to opt in to disease management.

Okay. We have basically given that up on the Senate side. You know, we have said that compelled authorization is going to include some treatment which will have some forms of disease management.

Now, we haven't given it up completely because it has to be tied to the individual, but we have been willing to live with the compromise. Why? Because the industry was willing to live with one thing. They took out the word "including" in your definition of health care operations. Right now health care operations is anything to the implement the terms of the contract—"including," and a whole list of the things. The minute you have the word "including," as a legal matter, you have no boundary. So there is a change that can be made in H.R. 2470 that can take care of that problem.

A much more difficult problem, and I only saw it 2 days ago—first time I saw this change—is that I think the industry had some concern about use and disclosure as it was done on the Senate side; and 2470 says that when a health plan or provider has protected health information, it can use that information for treatment, payment, health care operations and research. It can just use it.

Now, one effect of that is that they don't have to get an authorization, but to me that would have been a compelled authorization anyway. The bigger problem is that all of the rules of the law that apply to disclosure, how you have to be careful about disclosure, suddenly go out the window so long as it is a use for treatment, payment, health care operations and research. It is just a few legal words, and it completely undoes the rhetoric of what I understood you are trying to achieve.

Now, let me make a few comments on the three policy areas. One is research. We, of all groups, want research.

Who was it who said that her daughter is in a research trial?

Mr. BILIRAKIS. Ms. Capps.

Ms. FELDBLUM. We want research to work well, but we also want an incentive for researchers to use nonidentifiable data when that will be okay for the research. Now, we in CCD say there should be an IRB system. Section 208 of H.R. 2470 right now has just a completely internal review system with no standard. To me, that is like almost two ends of the spectrum.

It is worth looking at what a group that was sort of in the middle came up with, which was to have an equivalent level of review and accountability. They had some issues with IRBs, but they wanted an equivalent level of review and accountability. What is in 2470 right now isn't that. It can become that through negotiation and compromise, but it is not yet in research.

On private right of action, every single——

Mr. BILIRAKIS. Try to summarize if you can, Ms. Feldblum. We are all fascinated here, to be honest with you, but I guess I can't let it go on too long.

Ms. FELDBLUM. In private right of action, every privacy act that this Congress has passed has included a private right of action because if you ask any lawyer worth his or her salt, do you want criminal and civil penalties where you have to depend on someone else to have the resources to bring the case, or do you want a private right of action that you can go into court, any lawyer worth his or her salt, if they are trying to achieve effective remedies will ask you for the latter. So if you don't put that latter in, you are not creating the effective remedies.

And on preemption, again, I would recommend that you look to some of the compromises that had been worked out on the Senate side. We are not thrilled with it at the moment, but it is a movement that at least grandfathers in existing State laws and allows a carve-out for certain areas where it would by very problematic if you had a little vacuum cleaner preemption language, which is what you have, causing incredible, inadvertent consequences.

So I will conclude by saying I think this Congress can pass good, effective privacy legislation. It has been trying to do so for 20 years, and now in fact is the time you might be able to do it; but only, in my mind, if you build on the consensus and the compromise that has been happening over the last 6 months to a year, not start with something that is way back.

Build on the consensus that has developed already from different arenas. Work with all of us so it is in fact a bill that is bipartisan and is in fact a bill that is not just supported by industry but by consumers. I can guarantee to you today there is a bill that we can support and that industry can support, and that will make a difference for this country. You have to make sure that we get that opportunity to do that work together.

Thank you.

[The prepared statement of Chai Feldblum follows:]

PREPARED STATEMENT OF CHAI FELDBLUM ON BEHALF OF THE PRIVACY WORKING GROUP OF THE CONSORTIUM FOR CITIZENS WITH DISABILITIES

I. INTRODUCTION

My name is Chai Feldblum and I am a Professor of Law and Director of the Federal Legislation Clinic at Georgetown University Law Center. I am here today representing one of the Clinic's pro bono clients, the Consortium for Citizens with Disabilities (CCD) Privacy Working Group. Many members of the Privacy Working Group are also members of the Consumer Coalition for Health Privacy, an initiative of the Health Policy Project at Georgetown University. Indeed, the Chair of the Privacy Working Group—Jeff Crowley of the National Association of People with AIDS—is on the steering committee of the Consumer Coalition for Health Privacy.

CCD is a Washington-based coalition of nearly 100 national disability organizations that advocates with and on behalf of children and adults with disabilities and their families. All persons who receive health care services in this country have rea-

son to be concerned with the inappropriate use of highly personal information that is collected about them within the health care system. As a coalition representing people living with disabilities, however, CCD's views on this issue are somewhat unique. Because people with disabilities have extensive medical records and sometimes stigmatizing conditions, such individuals feel a particular urgency to secure new privacy protection at the federal level. At the same time, many people with disabilities interact on an almost a daily basis with the medical establishment and thus benefit from a well-run, effective health care system. Such individuals do not want federal privacy protection to reduce the effectiveness of the health care system they must navigate on an ongoing basis.

All of our work in this area has taught us that the desire for medical privacy and the desire for an effective health care system are neither in conflict with each other, nor do they require "balancing" of one interest against another. Rather, establishing privacy protection can *enhance* the operation of the health care system, by increasing individuals' trust and confidence in that system. A national survey released in January 1999 found that one in six Americans engages in some form of "privacy protective behavior" because he or she is afraid of confidentiality breaches regarding their sensitive medical information. These activities include withholding information from health care providers, providing inaccurate information, doctor-hopping to avoid a consolidated medical record, paying out of pocket for care that is covered by insurance, and—in some cases—avoiding care altogether.[1] None of this is good for either consumers or the health care system.

The CCD Privacy Working Group has developed a set of principles for health information privacy legislation designed to achieve the twin, mutually enhancing, goals of increasing privacy protection in the health care system and creating an effective health care system. The CCD Privacy Working Group has also worked with the Consumer Coalition for Health Privacy in the development of its principles. If there is no objection, I would like to submit these principles for the record.

Because the CCD Privacy Working Group believes it is imperative for Congress to pass federal medical privacy legislation, we have also worked diligently over the past several years to understand the concerns of *all* interested stakeholders in this area—including health care providers, health plans, pharmaceutical companies, researchers, public health departments, law enforcement officials, and state legislatures—to help bring about a consensus between our members and those stakeholders. We have done that work in two forums. First, as part of the federal legislative process, we have engaged in discussions and negotiations to help develop a consensus piece of federal legislation. Thus far, as a legislative matter, that work has primarily taken place with interested stakeholders under the aegis of the Senate Committee on Health, Education, Labor and Pensions, and has resulted in a proposed Senate Committee Chairman's mark to be offered by Senator James Jeffords. While the CCD Privacy Working Group has some remaining concerns with Senator Jeffords' legislation, we believe that legislation represents significant movement and consensus on the part of *all* interested stakeholders in this debate.

Second, Jeff Crowley, Chair of the CCD Privacy Working Group, participated in a year-long effort coordinated by the Health Privacy Project at Georgetown University. Under the leadership of Janlori Goldman, Director of the Health Privacy Project and a long-time privacy advocate and policy analyst, the Project convened a Health Privacy Working Group consisting of high-level representatives from disability and mental health groups, health plans, providers, employers, standards and accreditation organizations, and experts in public health, medical ethics, information systems, and health policy.[2] The mission of the Working Group was to "achiev[e] common ground on 'best principles' for health privacy and identif[y] a range of options for putting those principles into practice."[3] The Working Group was not intended to create a template for federal legislation. Rather, it was designed to create a set of "best principles" that providers and plans could voluntarily put into place even before federal rules were enacted. Thus, some key issues for the CCD Privacy Working Group that are unique to federal legislation were not addressed by that group (but will be addressed in this testimony). Nevertheless, on a wide range of issues—from rules regarding use and disclosure, to standards for authorization, to interaction with law enforcement—the Health Privacy Working Group

---

[1] California HealthCare Foundation, *National Survey: Confidentiality of Medical Records* (January 1999). The survey was conducted by Princeton Survey Research Associates. Results are available at www.chcf.org/conference/survey.cfm.

[2] Comprehensive member biographies are available as an Appendix to the Health Privacy Working Group Report. See Health Privacy Working Group, *Best Principles for Health Privacy,* at 46-50.

[3] *Best Principles,* at 12 (July 1999).

forged critically important agreements that may serve as guidance for Congress in the development of federal legislation. I would like to ask that a copy of that report be included in the record following my written testimony.

With these two experiences as background—the negotiations we have engaged in with various stakeholders at the federal level over the past four years, and the Health Privacy Working Group's discussions of the past year—we are pleased to offer you comments on H.R. 2470, the Medical Information Protection Act of 1999, sponsored by Representatives Greenwood, Shays, Norwood, and LaTourette, and H.R. 1941, the Health Information Privacy Act, sponsored by Representatives Condit, Waxman, Markey, Dingell, and Brown of Ohio. We are disappointed that H.R. 2470 fails to include many of the most basic provisions that *both* industry representatives and consumer groups were apparently willing to live with in a spirit of compromise and in a desire to move forward bipartisan, consensus legislation—as reflected in our respective public positions on Senator Jeffords' proposed committee mark. Thus, if anything, H.R. 2470 represents a step backwards from the significant movement that has been made over the past six months by all interested stakeholders. Nevertheless, perhaps because we are eternal optimists in the CCD Privacy Working Group—and certainly because we are committed to the passage of effective federal privacy legislation—we hope this hearing represents an honest and committed effort on the part of all members of the committee to consider changes to H.R. 2470 that will transform it into a bill that *is* capable of moving forward with broad bipartisan support.

The CCD Privacy Working Group would prefer that H.R. 1941 be the basis for legislative action, because that legislation already represents a process of negotiation and compromise among a range of views. Nevertheless, we believe that certain changes to H.R. 2470 would create a minimally acceptable bill that the CCD Privacy Working Group could support, rather than a bill that we must regretfully inform our members and the public represents such a serious threat to health care privacy that it should be defeated.

In this testimony, I will comment on almost all sections of both H.R. 2470 and H.R. 1941.[4] I hope this analysis will demonstrate to the Committee that there are only a few sections of H.R. 2470 that need to be modified in order to make the bill minimally acceptable. Of course, those changes deal with significant, and at times, contested policy determinations. Nevertheless, I believe our recommendations represent not only correct policy determinations, but I also believe—based on compromises we are willing to make in this legislation—that these changes are ones industry stakeholders should be able to agree to as well.

II. ANALYSIS OF H.R. 2470 AND H.R. 1941

The analysis of H.R. 2470 and H.R. 1941 uses the order of sections established in H.R. 2470.

A. Access to Records

H.R. 2470

Sec. 101. Inspection and Copying of Protected Health Information
Sec. 102. Amendment of Protected Health Information

H.R. 1941

Sec. 201. Right of Access
Sec. 202. Right of Correction and Amendment

Both the CCD Privacy Working Group and the Consumer Coalition for Health Privacy include the following as one of their principles for federal legislation:

> *Federal legislation should guarantee an individual the right to access his or her own health information and the right to amend such information.* Individuals should have the right to access and amend their own medical records so that they can make informed health care decisions and can correct erroneous information in their records.

This principle was also adopted as principle #3 by the Health Privacy Working Group.

Both H.R. 2470 and H.R. 1941 embody this principle. H.R. 1941 does so by providing individuals the right to inspect, copy, and amend their protected health information as set forth in the recommendations conveyed to Congress by the Secretary of Health and Human Services pursuant to the requirements of the Health Insurance

[4] Where the sections of the bills do not differ significantly from each other, and/or from CCD's principles, I have not presented an analysis of those sections. I would be happy to supplement my testimony, within the week, with an analysis of those sections as well.

Portability and Accountability Act of 1996 ("Secretary's HIPAA recommendations").[5] H.R. 2470 achieves essentially the same result by setting forth the rights and responsibilities of consumers, providers, and agents with regard to access and amendment. Although the CCD Privacy Working Group would prefer that there be explicit time limits in the legislation regarding requests for access and amendment, we find this section to be acceptable.[6]

B. Notice of Confidentiality Practices

H.R. 2470

Sec. 103. Notice of Confidentiality Practices

H.R. 1941

Sec. 204. Right to Notice of Information Practices and Opportunity to Seek Additional Protections

The Consumer Coalition for Health Privacy includes the following as one of its principles:

> *Individuals should be notified about how their medical records are used and when their individually identifiable health information is disclosed to third parties.* Individuals should be given written, easy-to-understand notice of how their individually identifiable health information will be used and by whom. With such notice people can make informed meaningful choices about uses and disclosures of their health information.

This same principle was adopted by the Health Privacy Working Group as Principle #4.[7] The Working Group noted that components of such notice should include: a description of how information will be collected and the information source (such as a medical record, treatment notes, and information from third parties); how the entity will use the information, and how, when, and for what purposes the entity will request patient authorization; what information the patient is permitted to inspect and copy and how to access such information; available steps, if any, to limit access and the consequences, if any, of refusing to authorize disclosure; the health care organization's policy for making disclosures with and without patient authorization (such as for research purposes, to law enforcement, for treatment purposes, etc.); and any other information relevant to the health care entity's data practices.

Section 103 of H.R. 2470 attempts to provide an adequate notice requirement, but fails in several regards. First, H.R. 2470 requires entities to post *or* provide notice of the entity's confidentiality practices. Posting notices is clearly not as efficient a means of informing consumers as would be providing notices to individuals in written or on-line form. For example, Senator Jefford's proposed committee mark requires that notice be posted and provided.

Second, the notice contemplated by H.R. 2470 includes notice of "the uses and disclosures of protected health information authorized under this Act." Unfortunately, because section 202 of H.R. 2470 allows entities to use a consumer's protected health information for treatment, payment, health care operations, and health research without ever obtaining an authorization from the consumer for such use, this part of the notice will presumably ring relatively hollow. The use allowed under § 202 is particularly broad in light of the fact that "health care operations" is defined in H.R. 2470 as any activity undertaken "to implement the terms of a contract for health plan benefits." Because there is no limitation as to *what* a plan can put into its contract, there is similarly no limitation on the types of activities the plan may engage in to implement those terms.[8] The open-ended definition of health care operations, combined with H.R. 2470's allowance of *uses* for such activities to be engaged in without even obtaining an authorization from the consumer, belies the title of this Act ("Medical Information *Protection* Act of 1999"). Because it is unclear to us whether section 202 was *intended* to have this drastic, adverse result (we certainly hope not), if section 202 is modified to create a more reasonable result, the notice

---

[5] Secretary of Health and Human Services, *Confidentiality of Individually-Identifiable Health Information* (September 11, 1997). Recommendations submitted to the Committee on Labor and Human Resources and the Committee on Finance of the Senate; and the Committee on Commerce and the Committee on Ways and Means of the House of Representatives pursuant to Section 264 of the Health Insurance Portability and Accountability Act of 1996.

[6] Our concerns with regard to parents accessing the records of their minors are dealt with in the sections on "next of kin" and "individual representatives."

[7] "Individuals should be given easy-to-understand written or on-line notice of how their information will be used and by whom." *Best Principles,* at 19.

[8] This definition stands in sharp contrast to Senator Jefford's proposed committee mark, which includes the *same* list of activities as "health care operations," but provides that health care operations means *only* those activities. To accommodate industry concerns regarding the possible future existence of necessary health care operations, the Jeffords bill includes within the definition of health care operations: "such other services as the Secretary determines appropriate through regulations (after notice and comment)." Sec.(4)(7).

section of H.R. 2470 (as well as the substance of the bill) will once again regain some meaning. (Such notice should, however, still be provided directly to the individual, as well as merely posted by the entity.)

The comparable provision in H.R. 1941, sec. 204, includes an explicit provision that a consumer be given "a reasonable opportunity to seek limitations on the use and disclosure of protected health information in addition to the limitations provided in such practices," and that the entity "obtain a signed acknowledgment from the protected individual acknowledging that the notice...has been provided to the protected individual." The reason H.R. 1941 includes these provisions is because it creates a system in which an entity is not required to obtain a prior authorization from the consumer in order to use the consumer's protected health information for purposes of treatment and payment. (See Sec. 301. Provision and payment for health care.) Although the CCD Privacy Working Group would prefer that a prior authorization be required, we have already agreed that health care providers and plans may be permitted to essentially *compel* such authorizations from the consumer by conditioning the delivery of service or payment on receipt of such authorization. Given that agreement on our part, the main purpose of a prior authorization for treatment or payment would have been to provide notice to the consumer of how protected health information would be used, and to provide that individual an opportunity to seek additional restrictions on use and disclosure. The provisions of section 204 in H.R. 1941 ultimately achieve those same two goals. Moreover, section 301(c) of H.R. 1941 also includes another essential component from our perspective: it allows an individual who pays for the care himself or herself to restrict disclosure to a health care payer of the protected health information created or received in the course of receiving such care. H.R. 2470 lacks this critical component (above and beyond the fact that it lacks any authorization at all for the "use" of health care information for payment purposes.)

C. Establishment of Safeguards

H.R. 2470

Sec. 111. Establishment of Safeguards

H.R. 1941

Sec. 104. Safeguards Against Misuse and Prohibited Disclosures

The Consumer Coalition for Health Privacy includes the following as one of its principles:

> *The development of security safeguards for the use, disclosure, and storage of personal health information should be required.* Appropriate safeguards should be in place to protect individually identifiable health information from unauthorized use or disclosure.

The Health Privacy Working Group also adopted, as Principle #6, that "health care organizations should implement security safeguards for the storage, use, and disclosure of health information." Although the Working Group did not discuss specific security controls at great length, there were a number of safeguards that were discussed in the context of "fair information practices." They included:

- Health care organizations should endeavor to limit access to personally identifiable health information on a need-to-know basis. Employers, for example, should endeavor to restrict access to personally identifiable health information strictly to those employees who need access for payment or treatment purposes.
- In keeping with Principle #1, health care organizations should remove personal identifiers to the fullest extent possible and practical, consistent with maintaining the usefulness of the information.
- All disclosures of personally identifiable health information should be limited to the information or portion of the medical record necessary to fulfill the purpose of the disclosure.
- Health care organizations should maintain a record of disclosures of information that identifies an individual.Personally identifiable health information should be used within an organization only when such information is necessary to carry out the purpose of the activity, for purposes reasonably related to the purpose for which the information was collected, and for which the patient has been given notice.
- Organizations should consider whether they are able to provide patients with a greater degree of anonymity in certain circumstances through the use of opt-outs, pseudonyms, identification numbers, or tagging information for additional protections.

It appears that the six subsections of § 111(b) of H.R. 2470 attempt to approximate some of these fair information practices and we applaud that effort. Unfortunately, however, until section 202's broad allowance of "uses" is modified, some of these safeguards will be useless. For example, § 111(b)(5) calls upon entities to have

an "appropriate mechanism for limiting *disclosures* to the protected health information necessary to respond to the request for *disclosure*." (This parallels the substantive requirement in §202(c): "Every *disclosure* of protected health information by a person under this title shall be limited to the information necessary to accomplish the purpose for which the information is *disclosed*.") But under §202(a), and repeated again for double clarity in §202(b)(1)(B), any use of protected health information for *treatment, payment, health care operations, and health research*—whether such use takes place within the entity or outside the entity—is *not a disclosure under H.R. 2470.*

The problem created by H.R. 2470 does not result simply from creating a distinction between "use" and "disclosure." Although members of the CCD Privacy Working Group have never understood, as a conceptual matter, why a distinction needs to be adopted between "use" and "disclosure," the simple creation of such a distinction does not—in and of itself—create a privacy problem. For example, the Health Privacy Working Group also assumes a distinction between disclosure (which it defines as "sharing of patient information outside an entity") and use (which it defines as "access or sharing of information within an entity, including to an agent or contractor of an entity.")[9] Then in its discussions of fair information practices, the Working Group apparently assumed that only "disclosures" of personally identifiable health information would need to be "limited to the information or portion of the medical record necessary to fulfill the purpose of the disclosure."[10] However, unlike H.R. 2470, the Working Group *also* assumed that personally identifiable health information would be "*used* within an organization only when such information is necessary to carry out the purpose of the activity, for purposes reasonably related to the purpose for which the information was collected, and for which the patient has been given notice."[11] By contrast, H.R. 2470 includes simply the weak statement, buried in the definition section of "disclosure" (section (2)(4)), that the use of protected health information shall not be considered a disclosure, "provided that the use is *consistent with* the purposes for which the information was lawfully obtained." Thus, again, H.R. 2470's rules governing use, as well as disclosure, must be revisited before the safeguards section of the bill can be assumed to mean very much to consumers.

The safeguards section of H.R. 1941 is stronger, primarily because the underlying bill is stronger with regard to the substantive protections for use and disclosure of personally identifiable health information. In addition, we prefer that the safeguards be required to include administrative safeguards to "ensure that protected health information is used or disclosed only when necessary," as H.R. 1941 requires, rather than having the safeguards simply "address the following factors," including "the need for protected health information and whether the purpose can be accomplished with nonidentifiable health information," as H.R. 2470 requires.

D. Accounting for Disclosures

H.R. 2470
Sec. 112. Accounting for Disclosures
H.R. 1941
Sec. 203. Right to Review Disclosure History

The Health Privacy Working Group includes, as part of its principle #3, that an individual should have the right to see "an accounting of *disclosures,* when such accounting is maintained" (emphasis added). This recommendation clearly does not assume there will be an accounting of all uses of health information within an entity. Similarly, both H.R. 2470 and H.R. 1941 require that an accounting be made solely of *disclosures,* and that such accounting be made available to consumers.

The CCD Privacy Working Group has no difficulty supporting H.R. 1941's (and the Health Privacy Working Group's) limitation of accounting solely to disclosures—because disclosures are defined in both H.R. 1941 and by the Health Privacy Working Group as providing access to protected health information to anyone *other* than an officer, employee, or agent of the entity holding the information. As a practical matter, it makes sense to require accounting solely of disclosures that occur *outside* an entity. Unfortunately, under H.R. 2470 a disclosure outside the entity is *still* not considered a disclosure for purposes of the law as long as it is a use for treatment, payment, the open-ended health care operations, or health research. Thus, in practice, the *only* accounting a health provider or plan will ever engage in will be for those *rare* situations in which disclosures are made for some purpose other than

[9] *Best Principles,* at 42.
[10] *Id.* at 22.
[11] *Id.*

these four broad areas. This radically restricts the entire concept of accounting for disclosures.

E. Restrictions on Use and Disclosure

H.R. 2470

Sec. 201. General Rules Regarding Use and Disclosure
Sec. 202. General Rules Regarding Use and Disclosure of Health Care Information
Sec. 203. Authorizations for Use or Disclosure of Protected Health Information Other Than for Treatment, Payment, Health Care Operations, or Health Research

H.R. 1941

Sec. 101. Restrictions on Use
Sec. 102. Restrictions on Disclosure
Sec. 103. Standards for Authorizations for Use and Disclosure
Sec. 301. Provision of and Payment for Health Care

Restrictions on the use and disclosure of protected health information lie at the core of any federal protection for the privacy of personally identifiable health information. Both the CCD Privacy Working Group and the Consumer Coalition for Health Privacy have stated a similar principle:

> *The use or disclosure of individually identifiable health information absent an individual's informed consent should be prohibited.* Health care providers, health plans, insurance companies, employers and others in possession of individually identifiable health information should be prohibited from using or disclosing such information unless authorized by the individual. Use or disclosure without informed consent should be permitted only under exceptional circumstances—for example, if a person's life is endangered, if there is a threat to the public health, or if there is a compelling law enforcement need. Disclosure of individually identifiable health information for marketing or commercial purposes should never be permitted without informed consent. Any time information is used or disclosed it should be limited to the minimum amount necessary for the use or disclosure.

The best way to ensure true informed *consent* on the part of the consumer is to allow an individual to *withhold* consent for use or disclosure of medical information, and still allow that individual to receive medical services without penalty. As a practical matter, however, health care providers and plans often need personally identifiable health information in order to carry out the business of providing treatment to the individual or reimbursement to providers. Given that reality, the CCD Privacy Working Group has agreed that authorizations for such purposes may essentially be compelled from the consumer by conditioning the provision of treatment or payment on the receipt of such authorizations. A key requirement, however, is that the consumer must be permitted the option of self-paying, and thus be permitted to retain the right to halt disclosure to a third party payer in such circumstances.

The Health Privacy Working Group similarly recognizes the practical requirements with regard to treatment and payment, but also recognizes another group of activities termed "core business functions." The Working Group agreed on the following approach:

> The Working Group agreed that, as a general rule, patient authorization should be obtained prior to disclosure. At the same time, patient information needs to be shared for treatment, payment, and core business functions. The Working Group agreed that the patient need only provide authorization for these core, essential uses and disclosures once. Furthermore, a health care organization can condition the delivery of care or payment for care on receiving this Tier One authorization. All other activities outside this core group must be authorized separately by the patient and health care services should not be conditioned on receiving this Tier Two authorization. The Working Group also agreed that there are additional, limited activities—such as public health reporting and emergency circumstances—for which patient authorization should not be required.[12]

Although the CCD Privacy Working Group has not issued a formal position on core business functions, we have stated that we find Senator Jefford's proposed committee mark on this issue to represent a minimally acceptable bill. Senator Jefford's bill is largely consistent with the consensus reached by the Health Privacy Working Group, although the bill uses a new term "health care operations," rather than the better, more established term of "core business functions." Nonetheless, given the definition of "health care operations" in the Jeffords bill, which establishes clear pa-

[12] *Best Principles,* at 22. The Working Group also agreed that "where a patient self-pays, he or she can refuse to authorize disclosure to a payer."

rameters for that term, the CCD Privacy Working Group is able to consider the Jeffords bill minimally acceptable in this area.

By contrast, H.R. 2470 diverges from any previous bill (including the bill introduced by Senator Robert Bennett, the bill which H.R. 2470 otherwise tracks in almost all respects), in rejecting the need for any authorization for use of protected health information in the areas of treatment, payment, open-ended health care operations, and health research. Instead of requiring an authorization, and instead of placing any real limits on the uses of personally-identifiable information in these four areas, H.R. 2470 offers the following simple, precatory language: "An individual who furnishes protected health information in the context of obtaining health care or health care benefits has a justifiable expectation that such information will not be misused and that its confidentiality [will] be maintained." Sec. 202(a). While this language is a nice piece of privacy prose, given that this is a piece of legislation, we would like to trade the prose for some actual statutory protection. The only protection offered by H.R. 2470, buried in the definition of "disclose," is that the use of protected health information shall not be considered a disclosure "provided that the use is *consistent with* the purposes for which the information was lawfully obtained." In light of the fact that a plan or provider may establish essentially any purpose as a "health care operation," this provides little solace to consumers.

Some of the industry stakeholders may not have intended the drastic cut-back in privacy protection that results from this new section in H.R. 2470. (Certainly, the Health Privacy Working Group which had a significant representation from industry espoused no such view.) The catalyst for this new provision may well have been the confusion regarding the rules for use and disclosure that some industry stakeholders perceived in Senator Jeffords' committee mark. The CCD Privacy Working Group does not believe either consumers or industry benefit from confusion with regard to use and disclosure rules. Hence, we greatly appreciate the effort of the Health Privacy Working Group to forge both consensus and clarity in this area. But the manner in which H.R. 2470 has dealt with this issue is truly horrific. It has removed any confusion regarding use of protected health information by removing any real *requirements* on such use. That cannot be the appropriate public policy determination. It certainly is not the position our 54 million members would recognize as a legitimate policy decision. We hope we can work with the committee to create a coherent and intelligent approach to issues of use and disclosure of protected health information.

F. Next of Kin and Directory Information

H.R. 2470

Sec. 204. Next of Kin and Directory Information

H.R. 1941

Sec. 307. Other Disclosures

Although disclosures of protected health information should ordinarily occur only pursuant to an authorization (compelled or real) executed by the individual, there are circumstances in which we would like health care providers to be able to disclose relevant health information to a select group of individuals who have a close relationship with the person who is the subject of the information. In such cases, we want to ensure the individual has been notified of his or her right to *object* to such disclosures, but if such an objection has not been lodged, we would like to ensure the provider may disclose relevant, current information.

Section 204 of H.R. 2470 essentially embodies this approach. As a technical matter, the section should refer to an "individual representative" as well, to include an individual who holds a power of attorney for another individual. In addition, the section should clarify that if a minor is legally permitted to receive a service without notifying his or her parent, that minor is also capable of lodging an objection to relaying protected health information regarding that service to the parent. (See discussion of minors below.)

G. Health Research

H.R. 2470

Sec. 208. Health Research

H.R. 1914

Sec. 304. Health Research

The issue of health care research—and the ability of large private companies to continue to engage in research that uses personally identifiable health information without first obtaining the informed consent of the subjects of the information—has been one of the most contested battlegrounds in the development of federal privacy legislation. In one respect, this should come as no surprise, given the millions of dollars expended and recouped as profit through such research. The issue is com-

plicated, however, by the mantra that "all research is good," and an accompanying assumption that we should create no possible hindrances to the development of new horizons of knowledge.

The CCD Privacy Working Group is acutely aware of the benefits of research. We are the ones that represent (and often are) the millions of people with disabilities who will benefit directly from public and private health research activities. Many people with disabilities live with conditions that are progressively debilitating, and, in some cases, fatal. Research leading to the development of new therapies or new habilitation and rehabilitation techniques can significantly enhance the quality of life for these individuals—as well as better ensure life itself. We want such research to proceed effectively and with full vigor.

We believe, however, that the best federal privacy law is one that ensures research activities will go forward effectively, will create incentives for researchers to use nonidentifiable information whenever possible and appropriate, and will create structures that will best protect privacy whenever identifiable data is necessary for a research project. Our proposal to achieve this kind of federal privacy protection is straightforward. If a health researcher is dealing with live individuals, the researcher should obtain informed consent from these individuals, pursuant to an authorization section of federal privacy legislation, before using such individuals (or their medical information or specimens) in a research project. Delivery of treatment or payment for services should never be conditioned on the receipt of such an authorization.

When research does not involve live human subjects, however, but rather involves medical records data or stored blood or tissue samples, it may not be feasible for a researcher to obtain the informed consent of the individuals who are the subject of the information. For example, some studies require researchers to review thousands of records for patients treated over a long period of time. In this instance, it would be quite difficult for a researcher to contact every individual whose medical records are contained in the database and ask for authorization to use their identifiable data.

In such circumstances, we believe the researcher—*whether that individual is using public funds or private funds for the research*—should consult with an institutional review board (IRB) to obtain a waiver of informed consent for those individuals whose protected health information will be used in the research project. We are well aware of the current limitations of the IRB system. Because the Common Rule that sets forth the guidelines for the IRB system was designed to focus on safety risks for human subjects, not on the confidentiality of data used in health research, the Common Rule currently provides little guidance for IRBs with respect to confidentiality. Thus, we believe a modification of the Common Rule would be necessary to ensure that informed consent and confidentiality standards are met by all research projects. Nevertheless, we believe it will be more efficient to modify the existing IRB structure rather than to attempt, through federal privacy legislation, to establish an entirely new oversight structure for confidentiality protections.

Despite our support for the IRB system, we believe Section 304 of H.R. 1941, which does not necessarily contemplate using the entire IRB system, meets the basic principles CCD seeks to achieve in this area. Our main concerns are that there be an *objective* process by which a determination is made as to the need for identifiable information in the research project and as to the lack of feasibility in obtaining informed consent; that there be some *accountability* through government oversight of such determinations; and that there be a *uniformity* in decisions about when, and under what circumstances, to grant a waiver of informed consent. H.R. 1941 achieves these goals by requiring that protected health information may be disclosed without an authorization for health research "only for uses that have been approved by an entity certified by the Secretary." Based on the Secretary's HIPAA recommendations, we can assume these entities will have some members who are not associated with the entity that wishes to conduct the research. Moreover, certification by the Secretary should allow for some opportunity for oversight, should potential problems arise. Finally, the determinations to be made by the entity (as set forth in the bill) can serve as the basis for uniform applications.

By contrast, Section 208 of H.R. 2470 has *no* requirement for objective oversight of research projects, *no* allowance for accountability outside the private entity, and *no* uniform standard for determining when research may be allowed to proceed without obtaining informed consent.[13] H.R. 2470 allows private entities that own

[13] Of course, under section 202 of H.R. 2470, protected health information in the possession or control of a health provider or plan "shall be available for use in health research that is not inconsistent with the requirements of other applicable Federal laws." A plain reading of this pro-

Continued

"protected health information previously created or collected" by such entity (presumably, pharmacy management plans may be some of the largest repositories of such information) to disclose such protected health information to a health researcher as long as: 1) the research has been "reviewed by a board, committee, or other group formally designated by such person to review research programs"; 2) the entity has an internal policy in place "to assure the security and confidentiality of protected health information" (this, of course, is already required under the safeguards section of the bill); 3) the entity enters into a written agreement with the recipient researcher "that specifies the permissible and impermissible uses of the protected health information"; and 4) the entity keeps a record of health researchers to whom the information has been disclosed.

All of these elements are certainly good, basic policies for any entity to have. It is striking, however, that the core elements that the Health Privacy Working Group—with its representation from both industry and research—identified as basic elements of privacy protection for research are completely absent from Section 208 of H.R. 2470. Some members of the Working Group were clearly not in favor of requiring IRB approval for all research given the limitations of the current IRB system. As the report notes:

> Concerns with the current [IRB] were significant enough, however, that members were open to using an alternate review process in situations where IRB approval is not currently required, *if it could offer the same potential benefits of the IRB system*... Where IRB approval is not required... a health care organization should have the option to either 1) obtain IRB approval *or 2) use an alternate process that provides an equivalent level of review and accountability.* (emphasis added).

As noted above, the position of the CCD Privacy Working Group is that IRB approval (assuming modification of the Common Rule) is the best approach. We are willing, however, to support a non-IRB approach that "provides an equivalent level of review and accountability"—assuming the promise of such a statement can truly be met. Section 208 of H.R. 2470 is a far cry from meeting that promise.

H. Law Enforcement and Oversight

H.R. 2470
Sec. 210. Disclosure for Law Enforcement Purposes
Sec. 206. Oversight
H.R. 1914
Sec. 305. Law Enforcement
Sec. 302. Health Oversight
Sec. 308. Redisclosures

Principle #9 of the Health Privacy Working Group is that "health care organizations should not disclose personally identifiable health information to law enforcement officials, absent compulsory legal process, such as a warrant or court order."[14] The Working Group recognized the situation is different when government officials have legally authorized access to information to engage in oversight and enforcement of the law. In those instances, the information obtained for oversight purposes should not be used against an individual patient in an action unrelated to the oversight.

Both H.R. 2470 and H.R. 1941 allow broad access for oversight purposes relating to health care fraud, or for accrediting purposes. Both bills, however, also ensure that protected health information about an individual that is disclosed during such actions may only be used against the individual in an action that is related to health care fraud.

With regard to law enforcement, H.R. 1941 presents a simple, yet elegant solution to the question of what type of legal process we should expect from our law enforcement officials. Section 305(a) states that protected health information may be disclosed to a law enforcement official "if the law enforcement official complies with the fourth amendment to the Constitution." Section 305(b) then explains that, in terms of applying the fourth amendment, "all protected health information shall be treated as if it were held in a home over which the protected individual has exclusive authority." In practice, this means a person's health information will be provided the same level of fourth amendment protection that a person's private suitcase would get were it sitting in a closet at the person's home. Law enforcement officials who wish to seize or search the suitcase must either receive the person's consent,

---

vision is that if research is not otherwise governed by the Common Rule, a provider or plan may use protected health information for such research without even going through the minimal requirements of Section 208.

[14] *Best Principles,* at 39.

or obtain a warrant. Similarly, if a law enforcement official wishes to seize or search an individual's protected health information, that official should either obtain the individual's consent or obtain a warrant.

Section 210 of H.R. 2470 goes some distance in requiring there be adequate legal process before law enforcement officials may search and seize protected health information. Unfortunately, allowing an "administrative subpoena or summons" to be sufficient to allow disclosure to law enforcement officials is extremely problematic given the lack of any real process or standards used in executing such summons. The reference to those documents should be deleted.

I. Individual Representatives

H.R. 2470

Sec. 212. Individual Representatives

H.R. 1914

Sec. 401. Specific Classes of Individuals

These sections of the two bills should not be controversial, but for the question of how and when parents may exercise the rights of their minor children under this law. The policy of the CCD Privacy Working Group is as follows. In most cases, we expect and want parents to exercise all the rights of their minor children under this Act. These include the right to authorize disclosures, access information, and sue on behalf of their minor children.

There are limited circumstances in which we believe the minor *child zhas the sole right to exercise the rights provided by the Act. These rare circumstances exist when the minor may legally* obtain a medical service without informing his or her parents of the receipt of such service, and where a provider is available who is willing to provide such a service to the minor. These limited circumstances tend to arise in medical services that deal with: reproductive health (contraception; abortion); mental health counseling; substance abuse treatment; and treatment for sexually transmitted diseases. Some states have passed laws that provide minors the right to access particular services on their own; in other states, common law or constitutional law provides a similar right to the minor. Whatever the source of the legal right, the CCD Working Group believes that if a minor has the right to access a service on his or her own, that minor also must have the right to control the flow of the protected health information generated through that service.

The CCD Privacy Working Group also believes it is not appropriate for a federal privacy law to upset state laws that may *constrain* the ability of a minor to access services on his or her own. For example, many states require that a minor must inform one parent before obtaining an abortion. (To meet constitutional requirements, these states also provide for a "judicial bypass" of this notification requirement under certain circumstances.) The federal privacy bill should not undermine the state law by allowing a minor to withhold information about the abortion from the one parent. For that reason, it is important that the bill provide that where a minor may *legally* obtain a service acting on her or his own, then (and only then) may the minor exercise sole rights under the Act.

Section 212 of H.R. 2470 states simply that "the rights of minors under this Act shall be exercised by a parent, the minor or other person as provided under applicable state law." This sentence is completely ambiguous on the question of whether a parent may exercise her right to access her child's medical records, in a case where the child does not desire the parent to have such access—*and* the *state* has determined the child may *legally* obtain the medical service without informing the parent. As a matter of preserving the state's decision making (as reflected in its statutory, common law, and constitutional law), the federal law should not be permitted to trump the state's determination on the minor's autonomy. The ambiguity in section 212 needs to be clarified to ensure that the status quo is maintained in the various states on the issue of minors' rights.

J. Remedies

H.R. 2470

Sec. 301. Wrongful Disclosure of Protected Health Information
Sec. 311. Civil Penalty Violation
Sec. 312. Procedures for Imposition of Penalties
Sec. 313. Enforcement by State Insurance Commissioners

H.R. 1914

Sec. 502. Enforcement

One of the principles of both the CCD Privacy Working Group and the Consumer Coalition for Health Privacy is as follows:

Federal legislation should establish strong and effective remedies for violations of privacy protections. Remedies should include a private rights of action, as well as civil penalties and criminal sanctions where appropriate.

It is a truism that a right without a remedy is no right at all. One of the most glaring faults in H.R.2470 is the absence of any private right of action on behalf of ordinary citizens in this country. Every other piece of privacy legislation passed by Congress—whether it covers banks, credit reporting, video rentals, or communications—allows private citizens to sue in court when they have been aggrieved by a violation of the statute.[15] Indeed, this is a basic hallmark of a range of legislation passed by Congress.

There is a good, practical reason why Congress—in a range of laws—has deputized "private attorney generals" by allowing individual citizens to sue when violations of laws have occurred. One of the goals of legislation is often to make a societal impact on a particular problem. For example, one of the goals of federal privacy legislation is to change the *norms* by which various stakeholders operate. Instead of having entities assume a project will always be implemented with the use of personally identifiable health information, we want all entities to "stop, think, and justify" before they use identifiable data.

The best way to ensure that entities experience an obligation to learn and comply with the law, and the best way to ensure that individuals who have been aggrieved by a violation of the law are made whole, is to provide individuals the opportunity to file a suit in court, prove their case, receive damages for harm suffered, and recoup attorney's fees if they prevail. Anything short of such a scheme will create a law that may (possibly) look good on paper, but will do little to help real people across the country.

K. Preemption

H.R. 2470

Sec. 401. Relationship to Other Laws

H.R. 1914

Sec. 503. Relationship to Other Laws

One of the final principles of both the CCD Privacy Working Group and the Consumer Coalition for Health Privacy concerns the issue of preemption. As both coalitions note:

Federal legislation should provide a floor for the protection of individual privacy rights, not a ceiling. Like all other federal civil rights and privacy laws, federal privacy legislation for health information should set the minimum acceptable standard. Federal legislation should not pre-empt any other federal or state law or regulation that is more protective of an individual's right to privacy of or access to individually identifiable health information.

Of all issues, this has been one of the most fiercely fought during the legislative process. Consumer groups, including the CCD Privacy Working Group, have stated vehemently that states must be provided the opportunity to continue to explore ways in which to better protect the privacy of medical information in their particular states. Most industry stakeholders have just as vehemently argued that they need (or at the very least, that they very much want) the ease of complete uniformity that sweeping federal preemption of state laws can provide them.

Given the perceived intractability of both sides on this issue, it is surprising that the beginnings of a compromise on this issue had begun to be developed through Senator Jefford's proposed committee mark. Under this approach, all existing state laws dealing with privacy of medical information would remain in place. For state laws enacted *after* passage of the federal law, however, those that dealt with access and amendment of information, authorizations for treatment, payment, and health care operations, and research would be preempted. The only exception would be for future state laws dealing with mental health.

While this compromise approach leaves both consumer groups and industry groups wanting something closer to their original stance, the only remaining issue in contention in this compromise concerns the status of future public health laws. As soon as that issue is resolved, there should exist a minimally acceptable compromise on preemption that all stakeholders can accept. That would be a truly miraculous result. Given how close we are to a compromise, it is truly unfortunate that H.R. 2470 returns to an old version of sweeping preemption that is disrespectful of the states and their citizens, that is unnecessary for the purpose of allowing industry to engage in effective business practices, and that will have a potential host of

[15] *See* Fair Credit Reporting Act of 1970; Right to Financial Privacy Act of 1978; Cable Communications Policy Act of 1984; Electronic Communications Privacy Act of 1986; Video Privacy Act of 1988.

unintended adverse consequences that will put the adverse, unintended consequences of ERISA preemption to shame.

III. CONCLUSION

Congress has spent twenty years thinking about, and sporadically working on, legislation to protect the privacy of medical information. This is clearly an issue that resonates with the American people: people are concerned that there is a lack of strong, clear privacy protection with regard to some of their most sensitive medical information.

Although work on a federal privacy bill has proceeded for over twenty years, there is a sense of possibility and momentum now. Congress knows if it does not act to pass privacy legislation in the near future, the Secretary of HHS will step into the gap with regulations that will address a range of the privacy issues. But there is no reason for Congress not to act—assuming it builds intelligently on the consensus that has developed over time among the various stakeholders in the debate.

The CCD Privacy Working Group urges this Committee to build on and strengthen the consensus that currently exists in the area of medical privacy legislation. In particular, we urge you to seriously study both Senator Jeffford's proposed committee mark and the newly-released report form the Health Privacy Working Group. The CCD Privacy Working Group does not agree with all elements of Senator Jefford's draft—significant issues regarding minors, the private right of action, and future preemption of public health laws all remain to be resolved. Yet that list of major concerns is significantly shorter than the list of major concerns we have with H.R. 2470. Moreover, there are other elements of Senator Jefford's proposed mark that do not conform to our principles, but which we are willing to accept in the spirit of compromise. We would urge this committee to build on the compromises that have been accepted thus far by both consumer groups and industry groups, and help draft a bill that can be endorsed by a bipartisan group of Members and a wide spectrum of interested stakeholders.

Mr. BILIRAKIS. Thank you, ma'am.

Well, I guess you have certainly verified the complexity of this entire issue. Let me just try to get a little basic here.

Dr. Norwood, of course, brought up the point of the flow of information across State lines, and I may or may not be able to get to that, but he or someone else will I suppose. That is very important.

Let me go to Mr. Nielsen. What would be the implications of, for example a real practical situation, female breast cancer patients being able to remove their patient information from a data base that tracks breast cancer treatment outcomes? I will make this a three-prong question: Would this incomplete information—and I think we would all agree it would be incomplete information—not only affect that individual patient who removed her information but all future victims of breast cancer as well because they would not be able to benefit from scientifically sound outcomes and research? And going further, if restrictions were put in place as per the Markey-Waxman confidentiality bills, et cetera, what would that to do to your ability to provide disease management programs like Justin's?

Mr. NIELSEN. Thank you, Mr. Chairman. Let me answer it generally first.

What you are describing is the oft-commented-on issue of opt-outs, with the ability of patients to direct the content of their medical record. We don't like that. We don't think it is in the best interest of patients. Rather than have opt-out provisions or something of that nature, we think bills that protect the privacy through strong penalties, through the requirement that entities deal with this internally through strong policies that protect privacy is by far the better answer.

To be responsive to your question, the particularities of your question, if those kinds of opt-out provisions were present, our ability to comprehensively do disease management, to comprehensively, adequately care for patients so that physicians had the full ability to know what a patient's condition is would be significantly compromised.

I think Dr. Tang would agree with that and perhaps ought to address the question, too.

Mr. BILIRAKIS. Dr. Tang.

Mr. TANG. I will be happy to. I think opt-out causes two levels of harm, one is to the patient and the other is to the rest of us.

Mr. BILIRAKIS. That goes with my question, right.

Mr. TANG. So the harm to the patient is, just as Mr. Nielsen mentioned, it is very hard to take care of a patient without complete information. For example, if one of the carve-outs was psychiatric information, what if I didn't know the psychiatric medication this patient was on and am about to prescribe something to which there would be an interaction, or what if the patient was on a psychiatric medication whose side effect was cardiac arrhythmias and that is what I am trying to treat.

For the rest of us, I might have an anecdote about Laetrile from maybe the early 1980's. Laetrile had a particularly nasty side effect, death, and we didn't have any randomized controlled trials, so we had voluntary reporting. So let us say we had several patients taking Laetrile and the ones who died didn't actually get to report their outcomes. Our data base—in a sense, they had been opted out—would be biased in favor of not having those serious side effects show up. Now, that is an extreme example, but in an ongoing way, we would like to measure the outcomes of all our interventions, new and old, and if some people opt out, we will be deprived of that information, and that will hurt everyone, including people like Justin.

Mr. BILIRAKIS. Ms. Feldblum, comment?

Ms. FELDBLUM. This is exactly the conversation we had among the disability folks, which is why we are seeing—as a minimally acceptable bill, we are willing to support over in the Senate side the Jeffords committee mark. Under that bill, there is essentially a compelled authorization for treatment. Okay. You have to sign the authorization in order to get treatment, and treatment includes disease management. Now, it is disease management for the individual, but there is no opt-out capacity. We are not opposing the bill because we can't opt out because of exactly all of these issues.

What we have been concerned about and therefore what is of concern with 2470 is that in the definition of health care operations there is a lot more than just disease management, and so the key thing really for us in terms of comfort level is to make sure that the parameters of what are in the compelled authorization are known to us ahead of time so that we can, in fact, have this conversation. And I think the industry understandably, you know, understood the need for the parameters. We understood their need that who knows what is going to happen 10 years from now in terms of some activity, and so an additional piece was added in to say that the Secretary could add in activities to health care operations after notice and comment, so you weren't freezing it in 1999.

So I don't think we have got a disagreement on the principle here. We still have a problem with one word in the bill.

Mr. BILIRAKIS. Yes, Doctor.

Mr. APPELBAUM. Mr. Chairman, on this opt-out issue, it seems to me that part of this issue is real and part is a red herring. The disease management piece of this seems to me to be a red herring. Disease management can't take place without the cooperation of the patient. If Justin weren't willing to log on every day, there would be no disease management, and so a requirement that patients give consent before disease management is initiated would have no effect whatsoever on its efficacy.

As far as large-scale data bases are concerned and the possibility of patients ultimately benefiting from the information that they put into those data bases, that is a real issue, but in our system we have always allowed patients to make the choice for themselves, even the choice whether or not to accept care, even if refusal of care would ultimately lead to their harm; and similarly, we would argue that patients should continue to have the right to determine whether or not these kinds of benefits are the benefits that they want with their medical record information, or for whatever reason they choose to opt out of that that, they should have the right to do so.

Mr. BILIRAKIS. Do you have anything to add to this, Ms. Pawklak?

Ms. PAWLAK. From a patient standpoint, if 9 years ago when my husband signed up with his medical insurance I had been given the option of checking off a little box to opt out, I can just about guarantee I probably would have. That could have had terrible consequences for us down the line when Justin was diagnosed with a disease that we did not know about.

No one knows the future. He was diagnosed with the disease. We would not have had available to us the things that have been made available to us and the improvement in his basic health that has been made available, because his medical history of having asthma was available to someone who had a program that could help us.

We don't know the future. Basically, I would hate to think that through lack of knowledge, I had closed any doors. I would prefer to leave the doors open so that further down the line when something came up, I was able to participate and my information was there for somebody who had more knowledge than me to be able to see it.

Mr. BILIRAKIS. You put it well.

Health care operations, Ms. Feldblum particularly emphasized that.

Mr. Nielsen, what is your definition of that? Do you define it the same way?

Mr. NIELSEN. Well, I am not frightened by the definition. I mean, I think clearly what Ms. Feldblum has indicated in terms of wordsmithing the definition, I think we would be willing certainly to entertain that, but as I look at the definition, I think from a statutory construction point of view, the word "including" indicates that this list of operations is in fact inclusive.

Most, if not all--and let me say all of them, in my view, are well understood in the industry; I think we know what we are talking

about. Anything that goes beyond those, unless you have patient consent, is going to be prohibited and going to be subject to sanctions. Health care entities' health plans have to do certain operational kinds of things. They can do and they should do the sort of disease management, that has just been testified to, that saves lives. I mean, we are talking about enacting kinds of procedures that are going to save lives, that are going to enormously improve the health care delivery of this country. We ought not to foreclose the ability to do that and even protect people against themselves.

Mr. BILIRAKIS. Thank you, sir. My time is up.

Mr. Brown.

Mr. BROWN. Thank you, Mr. Chairman, and I want to follow up on Mr. Nielsen's statement and Ms. Feldblum's energized testimony, if you will.

First of all, Mr. Chairman, if I could, I would like to ask unanimous consent to enter Mr. Dingell's statement in the record and any other members' statements.

Mr. BILIRAKIS. Without objection, the opening statements of all members of the committee are made a part of the record.

Mr. BROWN. Thank you, Mr. Chairman. Also, a letter to you and to me from the National Conference of State Legislatures on the State preemption issue.

Mr. BILIRAKIS. Without objection.

[The information referred to follows:]

NATIONAL CONFERENCE OF STATE LEGISLATURES
July 14, 1999

The Honorable MICHAEL BILIRAKIS
Chairman
Health and Environment Subcommittee
U.S. House of Representatives
Washington, D.C. 20515

The Honorable SHERROD BROWN
Ranking Member
Health and Environment Subcommittee
U.S. House of Representatives
Washington, D.C. 20515

DEAR REPRESENTATIVE BILIRAKIS AND REPRESENTATIVE BROWN: On behalf on the National Conference of State Legislatures (NCSL), I would like to take this opportunity to comment on proposals regarding medical records confidentiality.

NCSL firmly believes that states should regulate insurance. We oppose preemption of state law, but we understand the desire to establish a minimum standard in this area given that health information is transmitted across state and national boundaries. We also realize that Congress must enact privacy legislation by August 21, 1999, as set forth by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and we recognize that all of the current approaches set some type of federal standard. Given these factors, we believe that the privacy of health information is one of the few areas where it is appropriate for the federal government to set a minimum standard. Federal medical records confidentiality legislation should provide every American with a basic set or rights regarding their health information. These federal standards, in concert with state law, should be cumulative, providing the maximum protection for our citizens. Our mutual goal should be to that not one individual's health information is more vulnerable under federal law, than it was without it.

Preemption of State Law

Federal legislation should establish basic consumer rights and should only preempt state laws that are less protective than the federal standard. Unfortunately many of the proposals pending before Congress take a different approach.

NCSL is particularly concerned about proposals that would preempt all state laws "relating to" medical records privacy. The universe of state laws relating to medical

records confidentiality is extremely large and is spread across a state's legal code. For example, state laws regarding medical records confidentiality can be found in the sections of a state's code regarding: health, education, juvenile justice, criminal code, civil procedure, family law, labor and employment law. There is currently no compendium of state confidentiality laws. NCSL continues to work with Georgetown University where a major effort to produce such a compendium is underway. A blanket preemption of state law is virtually the same as throwing the baby out with the bath water.

Should Congress seek to pass federal medical record confidentiality legislation, NCSL firmly believes it should: (1) grandfather existing state confidentiality laws; (2) narrowly and specifically define the scope of the preemption, preserving issues not addressed in the federal proposal for state action; and (3) permit and encourage states to enact legislation that provides additional protections. If states are precluded in some general way from taking action in specific areas, there must be a mechanism for a state legislature to act if federal legislation adversely impacts the citizens in the state due to a technical error or to unintended consequences based on state-specific conditions.

Some proposals attempt to address the preemption issue through the inclusion of state legislative "carve outs." This approach attempts to identify all the areas that states would be permitted to continue to enact legislation. While well-intended, there is no way for states to know the full extent and impact of the preemption and carve-outs until the federal law has been implemented. NCSL and the National Association of Insurance Commissioners (NAIC) recommend that states be allowed to continue to legislate and regulate in any area that is not specifically addressed in the federal legislation. Below is language jointly supported by NCSL and NAIC:

> Nothing in this Act shall be construed as preempting, superseding, or repealing, explicitly or implicitly, any provision of state law or regulation currently in effect or enacted in the future that establishes, implements, or continues in effect, any standard or requirement relating to the privacy of protected health information, if such laws or regulations provide protections for the rights of individuals to the privacy of, and access to, their health information that are at least as protective of the privacy of protected health information as those protections provided for under this Act. Any state laws or regulations governing the privacy of health information or health-related information that are not contemplated by this Act, shall not be preempted. Federal law shall not occupy the field of privacy protection. The appropriate federal authority shall promulgate regulations whereby states can measure their laws and regulations against the federal standard.

Current State Legislative Activity

Since January 1999, 26 states have enacted laws regarding medical records confidentiality. Montana enacted comprehensive legislation addressing the activities of insurers and North Dakota enacted legislation that established comprehensive public health confidentiality standards. After years of debate, Hawaii enacted a comprehensive law that sets standards for the use and disclosure of both public and private health information. Most states enacted legislation building on existing state law or legislation focused on a specific issue. Six laws, addressing a wide variety of medical records privacy concerns, were enacted in Virginia during the 1999 legislative session. Other states that enacted legislation this year are: Arkansas, Colorado, Connecticut, Georgia, Idaho, Indiana, Iowa, Louisiana, Maine, Mississippi, Nebraska, Nevada, New Mexico, Ohio, Oklahoma, South Carolina, South Dakota, Tennessee, Texas, Utah, West Virginia and Wyoming.

Several of these new laws address issues that are not addressed in many of the federal proposals. For example, many states have laws establishing strict confidentiality standards for medical information in the possession of employers. These laws would make records from employee assistance programs (EAP) and workplace drug-testing results, protected health care information, subject to strict disclosure and reporting requirements. Several states have laws that set limits on how much a health care provider can charge an individual to make copies of their medical records. These laws, designed to help assure access, regardless of income, would be preempted under some proposals. These are but a few examples that illustrate both the breadth and complexity of the preemption issue.

I thank you for this opportunity to share the perspective of NCSL on this very important issue and look forward to working with you and your colleagues over the

next several months to develop a consensus approval that will provide basic medical records privacy protections for all Americans.

Sincerely,

WILLIAM POUND
Executive Director, National Conference of State Legislatures

cc: Representative Thomas J. Bliley, Jr.,
Representative John D. Dingell,
Members, House Commerce Subcommittee on Health and Environment

Mr. BROWN. The issue of health care operations, Ms. Feldblum, in understanding that 2470 allows for disclosure without a person's authorization for those health care operations, and I am as concerned as you are about the definition and activities it includes and that it lists that and not the activities that it excludes. Talk to me about some of those.

It seems that because of the language, marketing activities, do they fall under this definition, insurance writing, insurance underwriting, employer use other than treatment and payment? What other kinds of activities might that include?

Ms. FELDBLUM. Actually, the activities that are listed in the bill would not include sending something to an employer. It would not include sending something from marketing. I mean, Mr. Nielsen is correct when he says those are words, that he knows that this is what industry does and, if he is correct, that this is all that health care operations should be, then I think this is something that consumers unfortunately may need to live with in a bill. In other words, all of the principles from CCD are, if you are going to compel our authorization for something, it should be for treatment for us and for payment for us, because that is sort of how you are thinking consumer-wise.

The group that Mr. Nielsen was a part of that the Georgetown Health Privacy Project put together says you also need sometimes to compel authorization for core business functions, things that consumers may not be thinking about. Where we have come to in the terms of the CCD privacy working group is acknowledging that there are some core business functions, but that marketing is not one of them, giving information to employers is not one of them and that the things that are listed here, with the sole exception of health care education, which we have some concerns with, are things which if these were the only things that were compelled from the authorization, we could live with in the same way that we are living with it on a Senate bill that we are not opposing.

So the whole conversation here about disease management is really, I don't think, quite relevant.

The only issue really about disease management is about medicine compliance programs. When you have got a disease that is more stigmatized, HIV, mental health, do you want to get the letter or the phone call about "Did you take your medicine" without anyone asking you, "Did you want to be part of that program"?

So health care operations, the things that are here are not a problem so long as it becomes truly exclusive, and it is not enough to say, "I read it as inclusive" when the language says otherwise.

The bigger problem that H.R. 2470 did—and we have never seen this before; this is as of 2 days ago—is create this idea of use, create this idea of use, and say that if the health plan has some protected health information, it has it, if it uses it for treatment, pay-

ment, health care operations or research, that is it. There are no other limitations. All the limitations of the bill that apply to disclosures, accounting for disclosures, notice, safeguards, limit to the minimum amount necessary to achieve the purpose, all of those good rules don't apply anymore to use for treatment, payment, health care operations or research.

I mean, you already have a problem with how health care operations are defined. One can fix that with one word. You have to fix this new idea of use. And I understand where he was coming from, but, boy, the result is truly bad.

Mr. BROWN. So backing off—we are going back to health care operations for a moment and then exploring use perhaps later—we can fix that by specifically excluding marketing, excluding employer use beyond payment. We can generally fix that language similar to the way it is in the Condit bill, and also suggesting, maybe giving authority to HHS to explicitly down the road promulgate regulations so that future activities will continue to exclude that?

Ms. FELDBLUM. The main thing you need is to strike one word on line 18 on page 5. Doing that will mean that health care operations is only the things that you have listed, and you can pick up from the Condit-Waxman bill that describes the things that are not to be presumed as including. I don't think any lawyer would think they would be, but there is no reason not to make that clearer, and then in case there are future activities that might come up, you give the Secretary the authority to add those into his compelled authorization. That is how to fix health care operations. Then you move to the bigger problem of use.

Mr. NIELSEN. I think we are dealing with some semantical problems here. The way that I read this is that the list that is contained in the bill is in fact inclusive and it does provide those aspects that are permissible. It says nothing about marketing, for instance.

Mr. BROWN. So why would you not specifically—why would you not specifically then, if it is not so clear, make sure that it is clear and specifically exclude marketing and employees beyond that?

Mr. NIELSEN. I may not have a problem with that. The difficulty with the term "marketing" is what does it mean. Is that where for-profit hospitals or a plan is sending out reminders to do things which will clearly benefit them if the patient comes back? Is that marketing or are we talking about something more crass than that, where people are simply trying to reap competitive and commercial advantage. I don't have any significant problem with that kind of wordsmithing.

Mr. BILIRAKIS. I thank the gentleman. Mr. Greenwood.

Mr. GREENWOOD. I thank the chairman.

I think that Ms. Feldblum is correct, that all of the matters—many of the matters that we have discussed so far are manageable. We will get to the commonality there. The tough ones include the preemptions. Let me take the action of preemption, and I would like to ask Mr. Nielsen to describe for us the importance of preemption and then I would like to ask Mr. Appelbaum, if he would, to describe how he would achieve his goal, which is not to have pre-

emption, and satisfy whatever you think is legitimate about what Mr. Nielsen would describe as the needs for preemption.

Mr. NIELSEN. I have been at this for 3½ years now, and what we have diligently tried to do is to fill the void that currently exists in the dearth of privacy protections that exist in this country. Granted, there are some States that are far in advance of others, but a lot of States, maybe even the majority of them have no legislation whatever.

Mr. GREENWOOD. And those that do don't cover the ERISA.

Mr. NIELSEN. That is correct. It is beyond the scope of State regulation. What we are trying to do is achieve some sort of national standard that will guide and direct privacy throughout this country. It doesn't seem to me that privacy considerations in Oregon and California are any different than they are in New York and New Jersey. We are all Americans. We all share the same heritage and we all ought to have our records protected uniformly.

Now from a pragmatic standpoint, and we are an example but not an extreme example, we serve patients in three States. We serve a lot of patients in Utah that come from southeastern Idaho and southern portions of Wyoming. We need to deal with those States in a way that is consistent. If the different States have different privacy laws, it will be virtually—it will be extremely difficult, let me put it that way, to develop the kinds of data bases that we are doing unless those laws are consistent. The problem is significantly exacerbated here in the District, in the Northeast where you have a much greater concentration of people, where people live in one State and receive their health care in another.

And in the case of the District, you know the example here. We ought not have the patchwork that currently exists and will exist if we don't have a national standard.

One of the problems with some of the early iterations in the Jeffords compromise was that we ought to grandfather in all of the State laws, and then give the States an 18-month window of opportunity to enact laws. And after that everything is preempted by Federal law. That is an invitation for a rush to the State house for every State to enact privacy laws, and we are right back where we started. If we don't have a national standard, what are we doing here?

Mr. GREENWOOD. You have heard those concerns about the practicality of moving data across States and the way that could affect the cost of health care, and every time you raise the cost of health care, you reduce accessibility. If you can tell us how we achieve your goal, which is to allow the State to not preempt the States, and meet Mr. Nielsen's goal, you win the prize.

Mr. APPELBAUM. You haven't told me what the prize is going to be.

Mr. GREENWOOD. I haven't heard your response yet.

Mr. APPELBAUM. Mr. Greenwood, Federal legislation in any area is an awkward and slow-moving way of achieving change, and this area demonstrates that.

I think our concerns are not that there might not need to be in some areas, and regulation of ERISA plans is one example, some consistent Federal legislation because it is the only way to get at some piece of the problem. Our concerns deal with a blanket pre-

emption of State laws in all areas where it is unnecessary to achieve that change. Such preemption, it seems to us, would decrease or eliminate the ability of States to experiment in this area, would decrease the adaptability to local needs.

Mr. GREENWOOD. I think you are speaking a little more theoretically than I had hoped for. You referenced the result that safeguards would be unnecessarily removed. Can you give us an example of what would be unnecessary, in terms of removing a State law, to fulfill Mr. Nielsen's articulated needs to move information across State lines and serve people across State lines without a complete mish-mash of regulations?

Mr. APPELBAUM. Sure. We serve people in central Massachusetts from northern Connecticut, from Rhode Island and southern New Hampshire. Our laws are the Commonwealth of Massachusetts. The laws that govern our operations affect the jurisdiction in which we exist and work. There is no confusion about which laws we have to follow and no problems with moving information to—in the current system, moving information to primary care physicians in these other States.

I have yet to see any clear documentation that these problems that are alluded to actually exist as problems, because in my day-to-day experience they don't. You asked for a concrete example. In Ohio, for example, there is a statute that says that the medical records of a patient are the property and creation of the physician or the caregiver and that the physician or caregiver has the discretion to release the records in whole when a request comes in or to craft some more limited disclosure of information.

That legislation was recently relied on in Ohio to reject a policy of managed care companies that were managing workers' compensation disability benefits for complete copies of patients' psychiatric records, including their psychotherapy notes. That piece of legislation would be wiped out by a total preemption in a way that does not affect any of these broader needs which could be addressed by a more finely crafted bill.

Mr. BILIRAKIS. Thank you. Mr. Waxman.

Mr. WAXMAN. It seems one of the problems with States adopting different laws is that we do live in one country; but one of the reasons that States have adopted different laws is that we have no Federal standard. If we adopt a strong Federal standard, it seems to me there is no reason for States to want to adopt something that is weaker. They will accept this as a Federal standard. But if the States want to adopt something stronger, should we preclude them from doing so?

Dr. Appelbaum, you talked about the Ohio case. Some States have adopted valuable patient protections like saying there should not be access to verbatim psychiatric notes, and some other States are also looking at that. Is losing those kinds of protections the kind of thing that you are worried about?

Mr. APPELBAUM. Yes. Here in the District of Columbia, for example, there is a local provision exactly along the lines that you are referring to, that prevents the mandatory disclosure to insurers of managed care companies of psychiatric records for purposes of utilization review. That spoke to a local need, a need that was not and

would not be addressed by national legislation and a need that seems entirely legitimate.

I think we agree with you completely that were we to be adopting or talking about adopting Federal legislation at an extremely high standard of protection of confidentiality, there would be no need to allow States to go beyond that, but that is not what we are talking about. We are talking about compromises of a variety of sorts, and given that situation, we think that it is important to allow the States to protect their citizens to a greater extent.

Mr. WAXMAN. So it comes down to the question of whether we adopt the legislative compromise process something which would be a ceiling or which would be a floor. And if it is a floor, then I think most States will say that is where they are and they will accept it. But in some limited circumstances, States may feel that they want to go beyond it. The way that we approach it in the Condit-Waxman bill is to allow States to continue to enact stronger confidentiality protections.

Ms. Feldblum, did you want to add something?

Ms. FELDBLUM. I wanted to add, this is an example where the rhetoric is not matching up with the legal language. The rhetoric is that we are operating across all State lines and so we need uniformity. If you are in Massachusetts, you will do Massachusetts law, and in Vermont you do Vermont law. The only problem right now is if you are operating in 10 different States, you need to have your lawyer know those 10 different State laws. If you pass a Federal law, without saying a word about preemption, by the act of supremacy, you have created a uniform national standard. So whether you are in Connecticut, Vermont, Massachusetts, you look at that Federal law and that is your uniform standard and so you make it easier.

Mr. WAXMAN. I think you are being very helpful. Let's get a strong Federal standard. I think that will be the law of the land in most circumstances, and rarely will States want to act, but we will give them the ability to act when they feel they need to.

Moving to another topic, Mr. Nielsen, you are a member of this health privacy working group which released principles on which members reached agreement. One principle was that health care organizations should use an objective and balanced process to review the use and disclosure of personally identifiable health information for research. In contrast, the Greenwood medical records bill allows health care organizations to use an individual's health information for health research without the individual's consent and without any review process at all.

Do you believe that the Greenwood approach that allows use of personally identifiable health information for health research without any review meets the health privacy principles requiring an objective and balanced process to review the use of information for research?

Mr. NIELSEN. Let me answer it this way if I might. And I can do that by best explaining to you what we do in our institution, which we think probably is the correct way. Let me address it first generally. We do not believe that all research ought to be Federalized, that is all governed by the Federal common rule concept.

We have within our system, and I think the American Infomatics Association recommends the same thing, a data review or access committee which is a committee that is specifically designed to review that gray area between what is required under the Federal common rule and that which is archival research or internal research or, for that matter, other kinds of health care operations that deal with the dissemination of health information. I think the establishment of those kinds of internal review committees is a very important concept, and perhaps one that ought to be included within legislation.

But I want to emphasize that I do not believe that we ought to require that all kinds of internal operations that have to do with the use and disclosure of information and research that—where we are dealing with records that maybe isn't human subject research ought to be covered by a Federal IRB. It is just too cumbersome.

Mr. WAXMAN. Is it going to be an independent review? I would like to have Ms. Feldblum comment on that. You in the working group seemed to reach a consensus, but I am worried that Mr. Greenwood's approach on this takes us backwards and may lead us to self-interested internal review that may not be sufficient protection or even as good as what we now have.

Ms. FELDBLUM. Many of us believe that we should have the IRB system. John Nielsen is saying no. But that is the not the question.

The question is: Is there an independent equivalent review? There are two problems with H.R. 2470. One, in the research section, it is an internalized review system. It is unclear how you get the objectivity. So there is something that needs to be fixed in section 208 of the bill.

Second, use for research, it makes it sound like you don't need to go through section 208 if you are using it for research, so there is not even the internal review. I can't believe that you meant to do the latter because why would you want to make section 208 of your bill superfluous, but you have done it with those legal words.

Assuming you fix that mistake, section 208, how are you being consistent with what John Nielsen's group came up with, which is an equivalent—not IRB, they are very clear, they don't want it to be Federalized—but how about something that is more equivalent in terms of objective and balanced? I don't think that it is an insurmountable hurdle, but I think there needs to be some work to get there.

Mr. BILIRAKIS. The gentleman's time has expired.

Mr. Norwood.

Mr. NORWOOD. Mr. Chairman, we started out understanding that this was complex, and this panel is of great interest to me. I have listened to them carefully and unfortunately I agree with all of them, at least on some parts of what they are saying. If I might, I want to find out about who you are a little better. That may help my understanding.

Ms. Feldblum, if I ever need an advocate I want you to come work for me. At Georgetown University Law Center, how many lawyers are over there?

Ms. FELDBLUM. We have about 95 faculty.

Mr. NORWOOD. So, 95 lawyers?

Ms. FELDBLUM. And we train about 600 a year.

Mr. NORWOOD. How many are expert in health care policy?

Ms. FELDBLUM. We have about 10. We have actually one of the strongest health faculties in the country.

Mr. NORWOOD. Do you consider that center expert in all Federal legislation?

Ms. FELDBLUM. Oh, no. There is a lot of Federal legislation that gets passed—we are the largest law school in the country so we probably have the greatest expanse of expertise, but I am sure that we still don't cover all areas.

Mr. NORWOOD. You have made some very strong statements for which I tell you with all respect, I want you on my side. The problem with some of that is that if we were to put 100 lawyers in here, they would not agree with you at all. They wouldn't agree on anything, including the world is round, so we have to take what you are saying to us and be very careful with it, although you are very positive you are right.

I am sitting here thinking that I know two or three lawyers at the University of Georgia who will not agree and be an advocate against it just as well. I appreciate and admire your strong feelings, but from our point of view we have to be careful with what you are saying just in case there is another lawyer or two that might disagree with how you phrased with what is wrong.

So one of the things that I have learned up here, and I am proud I am not a lawyer, but I guarantee you this wordsmithing game is a game to let lawyers do anything they want to do and any bill they want to do it with in order to get done their agenda.

Mr. Nielsen, are you an attorney?

Mr. NIELSEN. I am, sir.

Mr. NORWOOD. I thought that probably was the case. Would you tell me a little bit about Intermountain Health Care?

Mr. NIELSEN. We were founded in 1975 when the Mormon Church divested itself of all of its hospital systems. They were determined to no longer be central to the mission, so a not-for-profit corporation was founded in 1975 which included the essence of that former system, plus others.

Mr. NORWOOD. Did you buy those hospitals?

Mr. NIELSEN. They were given to us and the company was formed with two goals. One, that no one should personally profit; and, second, that we should provide health care to anyone who needs it, irrespective of ability to pay.

Mr. NORWOOD. How many physicians do you have?

Mr. NIELSEN. We employ 400-plus. Plus on the health plan, we have affiliated physicians of about 2,500 others.

Mr. NORWOOD. Are they salaried positions when you say employed?

Mr. NIELSEN. They are.

Mr. NORWOOD. When they see a patient and document care as well as health care history, who owns that information?

Mr. NIELSEN. Well, the record itself is the property of the institution. The information, of course, is the individual's. We have always maintained that they are free to access that information if they need it for any reason.

Mr. NORWOOD. So that the paper it is written on belongs to you?

Mr. NIELSEN. That is correct.

Mr. NORWOOD. But the information in there should belong to the patient?

Mr. NIELSEN. Sure.

Mr. NORWOOD. With your 400 physicians—that information does belong to the patient. Why are you seeking that information in a central room somewhere with a big computer? Why do you want to compile all of that information that belongs to the patient, and what are you trying to get at by compiling it?

Mr. NIELSEN. We are attempting to establish a longitudinal data record of a patient's medical history that can be available to health care providers when they need it. For instance——

Mr. NORWOOD. About why can't health care providers simply call up Dr. Jones and say, Listen, I am treating this patient; send me over the record?

Mr. NIELSEN. Because Dr. Jones may be out of town. Dr. Jones may not be able to be immediately contacted. Rather than that kind of archaic kind of process, we have it instantaneously available to the physician. And let me give you an instance. A person presents themselves at the emergency room with some unknown malady, maybe a drug reaction, maybe something more severe than that. The emergency room physician can pull up that medical record instantly, know exactly what the medical history of that person is, what drugs he or she may have been taking to avoid prescribing or treating that individual inappropriately.

Mr. NORWOOD. Is there any other reason you want all of this information?

Mr. NIELSEN. You mean in a clinical setting or any setting?

Mr. NORWOOD. In any circumstance? Is there any other reason besides good health care that you want all of this information on computer? How many patients do you guys see? How many is in your network?

Mr. NIELSEN. We have almost 1 million covered.

Mr. NORWOOD. Is there any other reason you want that million patients and the health care information about them in your computer? And you are testifying before Congress, so careful here now; is there any other reason you want it?

Mr. NIELSEN. I can tell you, in all candor and honesty, our mission is to provide the very best possible health care to the people we serve and that statement would characterize why we are attempting to do what we are doing.

Mr. NORWOOD. You are a lawyer. Try again. Is there any other reason why you want that information? Of course you want good health care for your patients. That is a given. Any other reason you want it?

Mr. NIELSEN. There is no other reason other than to provide optimal health care. Now, that can be in the context of clinical delivery, it can be what health plans do in terms of disease management. But ultimately the goal is to provide the very best health care possible and that is the only reason.

Mr. NORWOOD. Of course. That is a given. Does it have anything to do with mathematical science? Do you favor outcomes as a way to help treat patients?

Mr. NIELSEN. Of course we do.

Mr. NORWOOD. Now that is the other reason, isn't it?

Mr. NIELSEN. If what you are getting at in terms of keeping an eye on physician practices to determine if in fact physicians are utilizing the best practice protocols and so on, as we measure outcomes against practices, yes, we use it for that purpose.

Mr. NORWOOD. I will tell you that is the best thing that you and all of managed care has done in this country today. You have taken a cottage industry and you have been able to put together mathematical results and outcomes and that is useful. The problem is, for the rest of out there, we worry that you depend on that way too much and less on medical science and the art of medicine.

Mr. BILIRAKIS. The gentleman's time has expired. Ms. Capps.

Ms. CAPPS. Thank you, Mr. Chairman. I will continue with my colleague's going through the panelists to get, you know, better.

Mr. BILIRAKIS. Ms. Capps, forgive me. We would like to get through this panel to give you the opportunity to go home and then we are going to break for an hour for lunch. I have a markup. Mr. Greenwood has a markup. And so when we say for lunch, it probably means that we won't be able to eat lunch, but we are going to break. I want to set a schedle for the benefit of the second panel so they can make their plans accordingly. I am sorry to interrupt.

Ms. CAPPS. I know that the American Psychiatric Association feels strongly about privacy protections and I know that the House of Representatives passed a financial services bill, H.R. 10, which contained medical records privacy protection. This bill was passed out of this very committee, and I would ask you to comment as you like on the medical records privacy protections in H.R. 10 and whether or not you believe this bill is adequate to protect patients.

Mr. APPELBAUM. As you know, we and 39 other medically related groups, including the American Medical Association, have expressed our concern about provisions in H.R. 10. This hearing demonstrates the complexity of this issue. To think that in their little more than a page of text, we might be able to implement confidentiality legislation that took all of these varying interests into account I think is a wonderful account but proved to be fruitless in its outcome.

In its broad sweep, H.R. 10 does away with requirement for consent notification about the use of their information by the insurance industry. It opens those records up in a widespread way to access, by law, enforcement entities. It allows internal use of this information for such tasks as marketing and others that were not envisioned by the people who provided this information to their insurance companies. There are no regulations governing secondary disclosures of this information. Once turned over under the provisions of this law, it would be free to be utilized in any way imaginable or unimaginable by the recipient. It would also preempt State regulation in this area, much of which is much more restrictive and more protective of patients' interests. I think those encapsulate our concerns.

Ms. CAPPS. And for me, that gives an urgency about this hearing and hopefully others that we will be having on this important topic.

Just to allow your expertise to further enlighten us, I understand that you over at the University of Massachusetts, Department of Psychiatry—what kind of safeguards does your institution put in

place to implement for privacy when you conduct research that we might learn from that?

Mr. APPELBAUM. All of our research is reviewed by our IRB under a general assurance that we provide to HHS regarding our research practices. We find this to be acceptable and a reasonable way of accommodating researchers' desires to gather data and patients' interests in privacy and protection of other sorts. As far as medical record information is concerned, our IRB, as I think most IRBs, uses a fairly straightforward approach.

To the extent that information is being gathered prospectively and patients can be asked for their consent in advance, their consent is solicited. To the extent that we are talking about accessing large medical data bases which have already been collected and for which it would be impossible to obtain for secondary utilization, that consent is not required as long as researchers build in confidentiality protections of their data. That has proven very workable.

And I might note that Mr. Nielsen's comments surprised me with the speed in which the value of a comprehensive Federal approach which covers the whole country disappeared as we moved from confidentiality legislation to protection of human subjects in research.

Ms. CAPPS. So that might be an example for us to include in our legislation?

Mr. APPELBAUM. Absolutely.

Ms. CAPPS. Are there others—would you feel that this would be a matter for preemption? That if we had this standard, that we could expect that this could be followed nationwide?

Mr. APPELBAUM. I would believe that this is a standard that could be followed nationwide and built on the existing common rule to which most research in this country already adheres.

Ms. CAPPS. Thank you.

Mr. BILIRAKIS. I thank the gentlelady. Mr. Burr, to inquire.

Mr. BURR. I thank the chairman. How quickly the chairman cleared the room of members with his announcement of lunch.

Let me go to another area and I really want to touch on what Mr. Waxman referred to. He suggested that it should be a Federal floor versus ceiling, and I will tell you that HHS couldn't define what they were doing as to whether it was a floor or a ceiling, and it has shifted as the debate has gone on, and so I know how that movement in the water feels, Ms. Feldblum.

And he questioned should we limit States from having the ability for stronger standards? Let me suggest to you that the determining factor in that answer should be, does it affect the health of patients?

I understand the group that you are in and I understand the group that you represent and I understand where you are coming from with the CRPs, and I understand from an industry standpoint the challenges that you are faced with. We have not concentrated much on the middle, but that is what the whole health care decision process should be based on, the human face right there.

And the question is how do all of the things that each one of you have brought up, how does Mr. Greenwood's bill and how does Mr. Markey's bill affect Justin? And that is really what I want to deal with because, Mr. Appelbaum, you have talked about an opt-out,

and that sounds very appealing to a patient, and I think you made a great statement that I would say I would do the same thing.

If uninformed when you signed up for your health plan, do you want your information released or held? Ninety-nine percent of the people in this room would hold it. And we would have very little information to do our clinical research from and clearly that would affect the health of the American people.

Is there a Federal need to talk about whether preemption is important? Yes, it is about the health of each individual patient, and that is one of the responsibilities for Congress. If not, we don't need to debate a patients' bill of rights or have a HCFA. There are a lot of entities that we can cut out, including the Food & Drug Administration, and the litany goes on and on.

So let's go to the heart of the opt-out, if we could. You feel that individuals should have the ability to opt-out of any of their records being used? Is that a correct interpretation on my part?

Mr. APPELBAUM. Yes, we believe that individuals should have control over their medical record information and decide when it is disseminated and when it is not.

Mr. BURR. Let me ask for a legal interpretation from Ms. Feldblum. If there is an opt-out like he describes, would a patient have the ability to opt-out from any of their records being shared with the FDA for the post-approval review of pharmaceuticals or medical devices?

Ms. FELDBLUM. You would have to modify that law to allow the person to opt-out. There is no bill that I know of that is allowing patients to opt-out of having their information——

Mr. BURR. I realize that. I am not on any of the bills. I am on some of the suggestions which have been made and I think the opt-out is one that—you are not the only one, Mr. Appelbaum, that have raised the individual power of the patient to say, I don't want my information to be shared, period, with anybody. An opt-out is fully opt-out or you opt in. You either share it or you don't.

My question is, under that from a legal standpoint, would that patient's information be illegal to be shared with the FDA who is federally charged with the responsibility to look at pharmaceuticals and medical devices after the approval period to determine whether there are adverse effects on health that may materialize from a larger tested population?

Ms. FELDBLUM. If you wanted that also to be illegal, you would have to amend that.

Mr. BURR. We would have to amend it.

Ms. FELDBLUM. You could not repeal the FDA law by implication by allowing someone to opt-out.

Mr. BURR. So how many places, if we did an opt-out, would we have to go back and change the bill to allow a valuable piece of information to be accessed when a person doesn't want it, because it is in the public interest and the public health interest versus the individual's choice up front?

Ms. FELDBLUM. That is one of the reasons that we are not suggesting that as a matter of policy.

I thought your point about preemption, the way to answer the question is to say how does it affect the individual person is the

best way to think about the question. Not convenience, not what is easier, but what is better for the patient.

And it seems to me that the first thing that is good for the patient is for Congress to do what it hasn't done for 20 years, which is pass a uniform national standard of privacy so that it doesn't matter whether you live in Kentucky or Massachusetts as to what your protections are. Then the second thing you should do if you care about the patient is if a State has decided that there is a particular problem that they have discovered that they want to legislate on for a particular person——

Mr. BURR. What if it is you coming to Congress saying we have determined something that ought to be Federal? Are we going to start raising the bar? Part of the system is the unpredictability of legislation as it relates to health care policy.

Ms. FELDBLUM. Nothing precludes you passing a Federal privacy law now, and 5 years from now somebody saying there is something else that should be done on a Federal level. The whole point about the States being the laboratories of experiments—it is better if you do it—and over the 5 years you discover that you were not completely brilliant, there is something you forgot, this way you leave an option for the States to fill in on the gaps, and you may decide 5 years later that you want to do it for the rest of the country.

Mr. BILIRAKIS. The gentleman's time has expired.

Mr. BURR. Let me just ask this question. Did Maine in their law get it right or wrong?

Ms. FELDBLUM. They got it wrong on next of kin.

Mr. BURR. So we are not the only ones that could get it wrong?

Ms. FELDBLUM. That is certainly true. But because of what Maine did, we will make sure that next of kin is done right here.

Mr. BILIRAKIS. Dr. Ganske.

Mr. GANSKE. Mr. Nielsen, you are a member of the health privacy working group?

Mr. NIELSEN. Yes.

Mr. GANSKE. And we got a report today in Congress Daily that you have made some progress on a number of issues and that you are releasing a report?

Mr. NIELSEN. It has been released. We have copies for everyone, I think. They are available.

Mr. GANSKE. According to Congress Daily, you have made some progress. Can you describe the group for the committee?

Mr. NIELSEN. Sure. It was comprised of people who are typically privacy advocates, disability advocates. It was comprised of clinicians, of industry people. I think the folks at Georgetown tried to get as broad a cross-section of individuals as they possibly could.

Mr. GANSKE. Ms. Feldblum, were you involved in this group?

Ms. FELDBLUM. Jeff Crowley, who is the chair of the working group for whom I am the pro bono counsel, was a member of this 15-member group. So I was involved in it via him.

Mr. GANSKE. So you are aware of what this report is?

Ms. FELDBLUM. Yes.

Mr. GANSKE. What is your assessment of that report?

Ms. FELDBLUM. My assessment is that it was a really good effort at trying to figure out best principles, and that in some areas it

will be very useful guidance to Congress about use and disclosure, authorizations, research. Even though it is—not all of the positions are ones that CCD holds, because it was a broad group, but some very useful consensus building on those issues. Not on all of the issues. They don't say anything about private right of action because it was not a template for Federal legislation, it was best principles for industry to do voluntarily. They can't create a private right of action so there are some issues that are unique to Congress that are not in this report, but there are a bunch. I think it is an awesome amount and an incredible amount of good faith and goodwill that went into this report.

Mr. GANSKE. And so the Consortium of Citizens with Disabilities is looking very favorably on this report?

Ms. FELDBLUM. There are things that are not addressed because there is not agreement. So preemption, private right of action we won't. But on other things, yes, we think it is very good.

Mr. GANSKE. I tend to agree with many statements made by members of the panel. I think that if you do set a strong privacy standard, that it tends to take away the necessity for States which have not already looked at this to come up with their own, and so it tends to create a national standard.

I happen to believe that States—in general, that States should not be preempted for stronger legislation. That is what I have looked at in terms of my own managed care protection as an example.

But that if you look at, for instance, the State of Iowa, we just passed some patient protections in the Iowa legislature, but had we had a pretty strong Federal law already in place, I don't think that the legislature would have picked it up.

So I am sympathetic to those who work across State lines in terms of having some uniformity. I think if we developed a strong enough privacy bill it would function that way, and at the same time I wouldn't want to preempt Texas or California for some of the things that they have done.

I have some problems with Mr. Greenwood's bill, that is why I am not a cosponsor, but I respect the work and effort that he has put into it.

Ms. Feldblum, I certainly appreciate how a few words can make a great big difference. We are dealing with a debate in the Senate right now on medical necessity where five little words would make a huge difference, and that is "not be bound by plan guidelines" that makes all of the difference in the world in terms of whether you have a strong bill or weak bill. Some of the things that you have pointed out in terms of this legislation are similar.

We are going to get down to some really difficult issues in terms of the enforcement. And I must admit as I look at the enforcement provisions in the bill that we are talking about today, I have some reservations about who actually would be subject to the criminal provisions. And then we are also going to have to get into, I think, a debate on the liability issue, and I haven't come to a decision on that yet either.

Ms. Feldblum, I am going to take advantage of the fact that I have a professor of law before me.

Have you looked at my provision, the Ganske provision in H.R. 10?

Ms. FELDBLUM. Yes, I looked at it about a week and a half ago.

Mr. GANSKE. I am going to do something that a trial attorney should never do, and that is to ask a witness for an opinion when you don't know exactly what they are going to say. But I want to clear up something about opt in and opt-out. An opt-in by my understanding is where you've got a provision that the information cannot be shared unless the patient gives the consent?

Ms. FELDBLUM. Right.

Mr. GANSKE. I thought we were getting a little bit confused when we were talking about that before. The provision that I had in H.R. 10 was an opt-in. It says the confidentiality of individually identified customer health, genetic information, the insurer may disclose that information only with the consent or at the direction of the customer, either with affiliates or outside of that health concern.

Then we had some specific provisions in terms of the standard underwriting and some things like that, but we say and here is an important word, at the end of that clause, "or as otherwise required and specifically permitted by Federal or State law."

Now, as a Georgetown lawyer on the faculty, is that not saying that this information or that this provision does not preempt State law as it relates to those exceptions?

Ms. FELDBLUM. Maybe I can write you something because I don't have the language in front of me. I will just say briefly, as I understood the problem with that, is the list of things that were exemptions before the "or" and whether some of that could be misinterpreted. My gut in reading it was it was intended to be very protective of privacy, and because of the point that Mr. Norwood made that there are some lawyers out there who would read things which is not what your lawyer intended it to be, that is the problem. I think this could be workable.

And for sake of time, I would want to get the exact question and I will commit to getting an answer in writing and orally as to what are the potential ways that language could be misused.

Mr. BILIRAKIS. The gentleman's time has expired.

Mr. GANSKE. One minute?

Mr. BILIRAKIS. We have to break in a few minutes. Thirty seconds.

Mr. GANSKE. It says also in compliance with Federal, State or local law. And then it says that this is enforced by the chief law enforcement officer of the State, the State insurance commissioner or otherwise, and so——

Ms. FELDBLUM. I will take that into account when I respond to your question.

Mr. GANSKE. Thank you.

Mr. BILIRAKIS. Mr. Markey.

Mr. MARKEY. Thank you very much, Mr. Chairman.

I do like the Ganske opt-in language. What I didn't like were the loopholes built into his exceptions which included: One, reporting to credit reporting agencies; two, disclosing information for research; three, disclosing information to insurance underwriters; and, four, disclosing information in connection with a merger or acquisition.

In itself it is the correct principle, but it is the loopholes that swallow the rule which cause the problem. I very quickly will go through the questions that I have.

On page 49 of the Greenwood bill, it says the disclosure of a person's protected health information is authorized for the purpose of reporting to consumer reporting agencies.

Why in the world should Equifax or some other consumer reporting agency get access to my most personal medical records? Once they get it, what safeguards are there from this information being accessed by others, including any company or creditor that I do business with, Ms. Feldblum?

Ms. FELDBLUM. Well, you know, this section on electronic payment cards, they always make a note that says superfluous, because they didn't really need a whole separate section for themselves. And you point out a problem that once you start putting in a separate section for someone, the fact is with all of these folks it should be done under the authorization. When I sign up for my credit card, I should have to file an authorization under section 203 which means that you can't condition my health care services——

Mr. MARKEY. It is kind of funny that this whole thing is in there. Why is it in there?

Ms. FELDBLUM. There was a lobbyist who convinced someone.

Mr. MARKEY. Let me move on to page 50.

Mr. GREENWOOD. If you know who that lobbyist is, will you let me know so we can meet?

Ms. FELDBLUM. I think it happened about 4 years ago.

Mr. MARKEY. There is an immaculate inclusion of this provision.

On page 50 it says banks, credit unions and securities firms are explicitly excluded from the requirements of the bill to the extent that they are engaged in transaction processing, functions described in subsection (b) of section 211 of the bill.

Furthermore, to the extent that banks or credit unions or securities firms are engaged in activities that fall outside the permitted activities in subsection (b), the bank regulations and the SEC are declared to be the exclusive enforcement agencies for such institutions.

The problem with that is neither the Federal securities laws nor the banking laws specifically empowers the SEC or the banks or credit union regulators to be health information privacy agencies.

I understand that the banking laws may give some kind of protection, the Fed and the credit union regulations may have some general authority to enforce against violations of any laws by banks or credit unions, but policing against such violations is not their primary mission. And the SEC has no authority in this area whatsoever so they couldn't take action against the securities firms that violated that section; is that right, Ms. Feldblum?

Ms. FELDBLUM. Well on page 51 what they say is nothing in the section shall be deemed to exempt the entities from the prohibition except (c). Subsection (c) says you can't disclose protected health information.

So what they have done is say you can't disclose protected health information, but we are not covering you under the bill for everything else, but do not construe that to mean that you can now disclose protected health information. It is another example of when

you start writing things specifically for individual industries, you really get in trouble because this is—this is a good teaching moment but a poor piece—poor drafting on this—is it so horrific, it is confusing.

Mr. MARKEY. But there is a reason that we use banks, credit unions and Equifax. All of these very interesting provisions built into——

Mr. BURR. Would the gentleman yield?

Mr. MARKEY. I will yield.

Mr. BURR. When you said for specific industries, would you also include the FDA? If you tried to write caveats for them, it might have different results on everybody else as well?

Ms. FELDBLUM. There is a section in here that says you can report to the FDA for the post-marketing problems. I have never felt that was a necessary provision. You could have put that in already by the overall system of when I authorize that compelled authorization, I also authorize for information to be going to the FDA.

You see, in other words there is so much—when you craft a bill correctly, you don't have to do a lot—all these other things.

Mr. BURR. Unless there is a blanket opt-out.

Ms. FELDBLUM. Yes, but we are not trying to do that.

Mr. BILIRAKIS. The gentleman's time has expired. Please proceed for another minute.

Mr. MARKEY. I thank you, Mr. Chairman.

The point that I am trying to make is that this bill has some good things in it. But again, I believe that much like the Ganske amendment, all of the exceptions swallow all of the good things, and you wind up with a product that is not ultimately consistent with public opinion, which demonstrates the passionate concern Americans have about not only their health care and financial and on-line privacy information generally. So it is an integrated kind of conversation here and it is difficult to go in any direction very long before you hit other areas, on-line, financial. And you have to have a uniform way of looking at all of this, so that we are agreeing on a set of principles, what it is that we want to accomplish, and regarding research and other areas, and we want to carve out things in other particular areas, but I don't think that we have reached that area on the committee. I think we are still grappling with the larger notion that everybody is entitled to the right to know the information being gathered about them, and the right to say no, you don't want it shared.

You can carve out some very specific and important public interest exceptions. But when banks, credit unions, Equifax, clearly are inside legislation, it is going to raise concerns. I hope that we can work together on a bipartisan basis because I think it is very important to work together on this, but I don't think that we have reached that point yet where we agree on the larger principle.

Mr. BILIRAKIS. The staff will be working very diligently starting at 5 o'clock this evening.

Mrs. Pawlak, because you are the only one here who basically has been directly concerned and involved in this, do you have any final statement that you would like to make, having heard all of this on both sides?

Ms. PAWLAK. A lot of what I have been listening to I have understood. A lot of what I have been listening to has been very confusing.

As a basic layperson, I have been involved in health care because of my son's illness. I have learned a little more about the health care industry. You are talking with a basic layperson who has not had the opportunity to learn more about it. You are talking to a person with less knowledge than I had on the subject, and in the case of the opt-out I would need somebody to protect me from me. I would have made a big mistake. Knowing a little bit about medicine, I would have made a big mistake. I need people who have more knowledge to protect me from me and protect my health from me.

Mr. BILIRAKIS. Well put.

The hearing is recessed until 1:45. Thank you very much. This panel is discharged. We ordinarily ask you if you are willing to respond to questions in writing. You all are, are you not? Thank you very much for being here.

[Whereupon, at 12:47 p.m., the subcommittee recessed, to reconvene at 1:45 p.m. This same day.]

AFTERNOON SESSION

Mr. NORWOOD [presiding]. Committee will come to order.

Let me first thank the witnesses for being here, and I will introduce you in just a second. We are in a very, very busy time right this minute, and many members will be back shortly, and I expect that we are going to be called to the floor in just a few minutes, but what I would like to do, if I may, is Mr. Waxman and I will introduce you, and we will at least begin the process so maybe you guys can get home sometime before dark tonight.

Our first witness is Ms. Carty, Cristin, Vice President of the California Health Institute. Thank you for being here.

Randy Johnson, Vice President of Labor and Employee Benefits, U.S. Chamber of Commerce; Dr. Andrews, who is Director of Worldwide Epidemiology, Glaxo Wellcome. Ms. Andrews, thank you for coming here.

Dr. Carolin Frey, Chairman of the Institutional Research Review Board. Thank you, ma'am, for being here.

And Dr. Greg Koski, Director of Human Research Affairs, Partners Health Care System. And thank you, sir, for coming.

We have already had one panel, and this is a most interesting and complex subject, and we appreciate all of you taking time to come and share your views with us. All of you have your information that will be in the record and submitted in the record, and Ms. Carty, if we could start perhaps with you, and we will try to limit these to 5 minutes, if we can.

STATEMENTS OF CRISTIN CARTY, VICE PRESIDENT, CALIFORNIA HEALTH INSTITUTE; RANDEL K. JOHNSON, VICE PRESIDENT, LABOR AND EMPLOYEE BENEFITS, U.S. CHAMBER OF COMMERCE; ELIZABETH B. ANDREWS, DIRECTOR OF WORLDWIDE EPIDEMIOLOGY, GLAXO WELLCOME INC.; GREG KOSKI, DIRECTOR, HUMAN RESEARCH AFFAIRS, PARTNER HEALTH CARE SYSTEM, MASSACHUSETTS GENERAL HOSPITAL; AND CAROLIN M. FREY, CHAIRMAN, INSTITUTIONAL RESEARCH REVIEW BOARD, PENNSYLVANIA STATE GEISINGER HEALTH SYSTEM

Ms. CARTY. Good morning, Mr. Chairman and members of the committee. Thank you for the opportunity to present testimony today on the very important topic of the confidentiality of patient medical information. My name is Cristin Carty, and I am the Vice President of Public Policy for the California Healthcare Institute. CHI's nearly 200 members including leading biotechnology, pharmaceutical, medical device companies and premier academic life science research institutions. Working on both the State and Federal levels, CHI strives to create a favorable climate for biomedical discovery and innovation, ensuring that patients have access to breakthrough therapies.

CHI supports the enactment of strong, uniform Federal standards, establishing accountability and penalties to protect the confidentiality of patient health information. Use of medical data should be restricted to activities that are deemed appropriate and necessary to quality health care and to research dedicated to improving health care outcomes.

Today, I will provide a snapshot of the bioscience industry in California and discuss the importance of framing one strong national standard that will secure all patient information equally.

Proposed new Federal regulations for handling medical information will clearly affect access to patients' medical data and, in turn, influence scientific progress. The challenge we face is to preserve the confidentiality of medical information without erecting barriers to the research that is our only hope to conquer diseases like Alzheimer's and breast cancer. In this context, I will touch on key provisions in the Medical Information Protection and Research Enhancement Act of 1999. Above all, I would like to encourage the adoption of a set of uniform Federal standards that will preempt conflicting State laws and thus safeguard scientists' ability to conduct crucial medical research.

Over the past 20 years, California has become the global headquarters for biomedical innovation. Overall, more than 2500 biomedical companies and 75 university and private research institutions are actively engaged in biomedical R&D, and health care technology now accounts for more than 200,000 California jobs.

Sound research and clinical testing is the cornerstone of inventing safe and effective new therapies. Essential to this process is a researchers' ability to utilize the full scope of patient data. The flow of medical information in a responsible and protected manner has played a vital role in the biotechnology revolution that has transformed medicine and that holds tremendous promise for scientific progress.

In 1997 alone, California's leading medical technology companies invested nearly $11 billion in research and development. It typically takes more than 10 years and $500 million to bring a new molecular entity from the laboratory to the bedside. New layers of restrictions on using crucial medical information will simply make what is already a very time-consuming and resource intensive process even more so, delaying new therapies and adding greatly to their already high cost.

California's leading edge biomedical companies are currently exploring scientific areas that raise important and complex questions regarding the confidentiality of medical information. These include basic research on human genome sequencing, the capacity to place DNA information in digital format, research into stem cells that will help scientists understand the causes of cell aging and death, and advanced diagnostics that will clearly target and enhance the use of therapies. In each of these areas, science is driven by patient medical data, including genetic information, ushering in a new era of medical promise.

Consider this example: Last September, the FDA approved a breakthrough treatment called Herceptin. The treatment was approved for use in patients with metastatic breast cancer who have tumors that overexpress the HER2 protein. In this case, research involving patient information, including genetic information, and the conduct of broad clinical trials helped scientists determine that the treatment was most effective for a specific population group, those who overexpressed the HER2 protein. Establishing uniform Federal standards for the treatment of all patient health information, including genetic information, will have a tremendous positive impact on future treatment advances. Conversely, if States continue to enact legislation that impedes the responsible flow of medical information, many potential new therapies will simply not be developed.

While guidelines to protect the patient's confidentiality are absolutely essential, the ability of the researcher to compile and access the medical data, governed by uniform and workable rules, will drive the pace and quality of crucial research.

As a State-based organization, CHI is highly attuned to the legislative developments in Sacramento. Recent attempts at the State level to legislate medical confidentiality, as well as broader privacy requirements, now threaten the cycle of biomedical innovation that has thrived in California. For example, some State legislators have discussed modeling State confidentiality regulations based on the European Union's data directive requiring unambiguous consent each time data is accessed and barring many uses of the data. Such a model would simply paralyze the important flow of medical information needed to fuel medical progress.

Drug studies depend on research throughout the country, and companies enter into partnerships with academic institutions and research entities in almost every State of the Union. Again, absent a uniform Federal standard as set forth in the Greenwood bill, a multitude of State requirements for the handling of patient health information could disrupt patient care and restrict the development and access to advanced medical technologies.

Finally, I would like to stress the importance of defining protected health information in precise legislative language. Researchers must be able to use nonidentifiable information for outcomes research, disease management programs, epidemiology studies and disease control.

Mr. Chairman, thank you for the opportunity to testify today. CHI's members are committed to the establishment of uniform Federal safeguards for the handling of medical information that promote accountability and are enforced by penalties. With these Federal guidelines, patient information will be protected and used responsibly. Also, with one uniform set of rules, medical progress in the areas of biopharmaceuticals, medical devices and diagnostics will continue at the pace we all have come to expect.

Thank you.

[The prepared statement of Cristin Carty follows:]

PREPARED STATEMENT OF CRISTIN CARTY, VICE PRESIDENT, PUBLIC POLICY, CALIFORNIA HEALTHCARE INSTITUTE

Good morning, Mr. Chairman and Members of the Committee. Thank you for the opportunity to present testimony today on the very important topic of the confidentiality of patient medical information. My name is Cristin Carty, and I am the Vice President of Public Policy for the California Healthcare Institute (CHI). CHI's nearly 200 members include leading biotechnology, pharmaceutical, medical device companies and premier academic life science research institutions. CHI is a non-profit, public policy research and advocacy organization for California's extensive health care technology enterprise. Working on both the state and federal levels, CHI strives to create a favorable climate for biomedical discovery and innovation, ensuring that patients have access to breakthrough therapies.

CHI has been working with key partners in the industry including the Pharmaceutical Research and Manufacturers of America (PhRMA) and the Biotechnology Industry Organization (BIO) on the many legislative proposals that have been drafted in response to the requirements outlined in the Health Insurance Portability and Accountability Act (HIPAA). CHI supports the enactment of strong, uniform federal standards, establishing accountability and penalties to protect the confidentiality of patient health information. Use of medical data should be restricted to activities that are deemed appropriate and necessary to quality health care, and to research dedicated to improving health care outcomes.

Today, I will provide a snapshot of the bioscience industry in California and discuss the importance of framing one strong national standard that will secure all patient information equally. Proposed new federal regulations for handling medical information will clearly affect access to patients' medical data and, in turn, influence scientific progress. The challenge we face is to preserve the confidentiality of medical information without erecting barriers to the research that is our only hope to conquer diseases like Alzheimer's and breast cancer. In this context, I will touch on key provisions in the Medical Information Protection and Research Enhancement Act of 1999. Above all, I would like to encourage the adoption of a set of uniform federal standards that will preempt conflicting state laws and thus safeguard scientists' ability to conduct crucial medical research.

Over the past twenty years, California has become the global headquarters for biomedical innovation. Overall, more than 2,500 biomedical companies and 75 university and private research institutions are actively engaged in biomedical R&D. Healthcare technology now accounts for more than 200,000 California jobs. More than 160,000 Californians are directly employed by organizations developing therapeutics and diagnostics, and manufacturing medical devices. Major universities, federal facilities and private research institutes employ an additional 44,000 Californians in biomedical and clinical research.

Basic and clinical research staff at California's nine leading university medical centers, UCSD, UCSF, UCLA, UC Davis, UC Irvine, Charles Drew University, Stanford, USC and City of Hope are involved in a full spectrum of investigation, from basic genomics to human clinical trials that test the safety and efficacy of new medicines and devices. Outstanding private research institutions like The Salk Institute and The Scripps Research Institute further contribute to an environment that fosters medical innovation and discovery. The research and clinical trials performed at

these state-of-the-art centers are fueling the development of powerful new technologies to treat patients.

Sound research and clinical testing is the cornerstone of inventing safe and effective new therapies. Essential to this process is researches' ability to access the full scope of patient data. The flow of medical information in a responsible and protected manner has played a vital role in the biotechnology revolution that has transformed medicine and that holds tremendous promise for scientific progress. The average biotechnology company spends half of its operating expenditures in the development of new products for unmet needs. In 1997 alone, California's leading medical technology companies invested nearly $11 billion in R&D. It typically takes more than ten years and $500 million to bring a new molecular entity from the laboratory to the bedside. The bulk of these resources are invested in the later stages of drug development, when a new medicine is subjected to extensive trials in humans. New layers of restrictions on access to this crucial medical information will simply make what is already a time-consuming and resource-intensive process even more so—delaying new therapies and adding greatly to their already high cost.

I know that during a previous hearing you heard from at least two expert witnesses who have first-hand knowledge of medical records-based research—Dr. Steven Jacobsen from The Mayo Foundation and Dr. John Curd who is now with VaxGen. Accordingly, my comments will be limited to two areas: patient information and its vital contribution to medical advances, and how uniform national standards, as exemplified in the Greenwood bill, will help preserve and even expedite the current pace of scientific discovery and development.

California's leading-edge biomedical companies are currently exploring scientific areas that raise important and complex questions regarding the confidentiality of medical information. These include basic research on human genome sequencing, the capacity to place DNA information in digital format, research into stem cells that will help scientists understand the causes of cell aging and death, and advanced diagnostics that will clearly target and enhance the use of therapies. In each of these areas, science is driven by patient medical data, including genetic information, ushering in a new era of medical promise.

Consider this example. Last September, the FDA approved a breakthrough treatment called Herceptin. The treatment was approved for use in patients with metastatic breast cancer who have tumors that overexpress the HER2 protein. In this case, research involving patient information, including genetic information, and the conduct of broad clinical trials helped scientists determine that the treatment was most effective for a specific population group—those who overexpressed the HER2 protein. Establishing uniform federal standards for the treatment of all patient health information, including genetic information, will have a tremendous positive impact on future treatment advances. Conversely, if states continue to enact legislation that impedes the responsible flow of medical information, many potential new therapies will simply not be developed.

One need to look no further than the National Institutes of Health (NIH) database to understand the full scope and promise of clinical testing research. With about 900 clinical studies under way at the NIH Bethesda location covering dozens of diseases and disorders, protocols are approved by review boards for ethics, safety, design and significance.[1] While guidelines to protect the patient's confidentiality are absolutely essential, the ability of the researcher to compile and access the medical data—governed by uniform and workable rules—will drive the pace and quality of crucial research.

As a state-based organization, CHI is highly attuned to the legislative developments in Sacramento. Recent attempts to legislate state-based medical confidentiality as well as broader privacy requirements now threaten the cycle of biomedical innovation that has thrived in California. Under the state's Confidentiality of Medical Information Act, medical records are considered private, and release of patient medical information is restricted absent patient consent. State proposals designed to amend this act and other sections of the California Civil Code could establish significant barriers to biomedical research. A bill offered in the state Senate last year would have prohibited "sharing" of biometric identifier information—defined as any "biologically based characteristic unique to an individual."[2] The bill was targeted at the financial services industry; however, it would have had the unintended consequence of ending most clinical research in the state. Pending bills raise a host of troublesome issues that will directly impact the quality of health care a patient receives. Two leading proposals, Assembly Bill 62 (Davis) and Senate Bill 19

[1] From the NIH website, The NIH Clinical Center, last best hope, www.cc.nih.gov/ccc/best/hope.html

[2] California State Senate Bill 1622, introduced Feb. 12, 1998

(Figueroa) are broadly drafted and may again create unintended results. For example, both bills may interfere with care coordination, case management and disease management models of care for persons with special health care needs such as the elderly, the disabled and the chronically ill. Senate Bill 19 would also permit an omnibus category of "contractors"—whether custodian, data processor or researcher—to disclose medical information in certain circumstances. In addition, other state legislators have discussed modeling state confidentiality regulations based on the European Union's data directive requiring "unambiguous" consent each time data is accessed and barring many uses of the data. Such a model would simply paralyze the important flow of medical information needed to fuel medical progress.

Drug studies depend on research throughout the country, and companies enter into partnerships with academic institutions and research entities in almost every state of the Union. Although the California Legislature has yet to fully approve the proposals mentioned above, it is important to convey the full scope of legislation being considered on the state level. Legislation passed in Minnesota restricts access to medical records for research purposes. Dr. Curd has already testified on this topic, citing how the Minnesota law "has made it more difficult for the Mayo Clinic to conduct epidemiologic research by requiring specific patient authorization for the use of patient data." Aside from the bureaucratic challenge of complying with medical information confidentiality requirements on a state-by-state basis, a patchwork of laws would also influence the types of populations included in clinical research—perhaps dissuading research into certain sub-populations. Again, absent a uniform federal standard—as set forth in the Greenwood bill—a multitude of state requirements for the handling of patient health information could disrupt patient care and restrict the development and access to advanced medical technologies.

Finally, I would like to stress the importance of defining protected health information in precise legislative language. It is absolutely essential to understand that nonidentifiable information—information that is coded or encrypted or otherwise made anonymous (and thus cannot be connected with an individual)—is essential to health research. Legislation should reflect that such data does not raise privacy concerns. Researchers must be able to use nonidentifiable information for outcomes research, disease management programs, epidemiology studies and disease control.

Mr. Chairman, thank you for the opportunity to testify today. CHI's members are committed to the establishment of uniform federal safeguards for the handling of medical information that promote accountability and are enforced by penalties. With these federal guidelines, patient information will be protected and used responsibly. Also, with one uniform set of rules, medical progress in the areas of biopharmaceuticals, medical devices and diagnostics will continue at the pace we all have come to expect.

Mr. NORWOOD. Thank you, Ms. Carty.

Mr. Johnson

STATEMENT OF RANDEL K. JOHNSON

Mr. JOHNSON. Thank you, Mr. Chairman.

Mr. Chairman, I have been asked to address the narrow, but critical issue of whether or not a private cause of action in court should be authorized under the legislation before you today. We believe, representing the U.S. Chamber of Commerce, that the only reasonable answer to this question is no, and the Chamber would strongly oppose inclusion of a new individual right to sue in addition to the severe criminal and civil penalties already in the legislation.

Contrary to the assumptions of some, it is not true that a new right to sue must or should be created each time Congress creates a new substantive legal right or that such a right is necessary for effective enforcement—although it might be necessary to keep the 600 lawyers that Ms. Feldblum referred to who graduated from Georgetown employed.

Furthermore, experience would suggest that given the inherent negatives associated with court litigation, Congress should reserve creation of a new, private cause of action in court for only those sit-

uations where there has been a demonstrated and well-documented problem with existing enforcement mechanisms. This threshold criterion has not been met here, obviously.

It should be emphasized that whatever is enacted will be an important but complicated law as evidenced by the prior panel. Before we subject individuals and organizations to the expense and uncertainty of private litigation, we need to allow some time for any uncertainties in the law to be clarified. Hopefully, much of this will be accomplished through administrative regulations which are provided for in this legislation by HHS that will flesh out the many rights, responsibilities and protections, a far preferable course to the vagaries, expense and inconsistencies of the court system developing policy on a case-by-case basis, depending on what circuit you happen to be in.

And since the question of whether a private cause of action is necessary, I think turns on obviously what deterrence is in the legislation right now, I would urge that the members take a careful look at the actual proposal, starting on page 55. Let us take a look at the criminal penalties first.

Now, under this section, a person—and a "person," by the way, is quite broadly defined in this legislation—a person that knowingly and intentionally discloses protected health information shall—shall, not may—be fined up to $50,000, imprisoned not more than 1 year or both, and if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned up to 5 years or both. If the offense is committed with the intent to sell, transfer, or use protected health information for monetary gain or malicious harm, the person could be fined up to $250,000 and imprisoned not more than 10 years or both. All of these penalties and prison sentences could be dealt with under certain circumstances.

Again, I note that the person who was subject to these fines and criminal imprisonment is defined quite broadly in the act. You may want to look at the definition part on page 11. It apparently includes anybody from a clerical worker up to a top guy in the business. Hence, the sweep of the provisions are quite encompassing.

Now, let us take a look at the civil penalties under 311. Any person, again, whom the Secretary of HHS determines has substantially and materially failed to comply with the act shall—not may—shall be subject up to $500 for each violation and up to $5,000 for multiple violations under Title I, and where a violation relates to Title II, a civil penalty of up to 10,000 for each violation and up to $50,000 in the aggregate for multiple violations. A $100,000 penalty is provided for violations which constitute general business practice. Injunctive relief is also provided for.

Now, I want to emphasize this point. To state the obvious, I can assure you that any entity, any person covered by this legislation is going to take these civil and criminal penalties quite seriously, and I have to ask if there is anyone in this room, including on the dias today, who would view these possible jail terms and monetary penalties lightly if they were subject to this law? I doubt it, and I would ask you for one moment to put yourself in the place of an individual within a business handling health care information of whatever size and ask yourself that question. Given the complexity of this law, I think some people might say, the regulated commu-

nity, well, better you than me and good luck and God bless. And too often that is the problem.

Now to help demonstrate the extreme nature of these criminal penalties and civil penalties, it might be useful for the purposes of comparison to look at a few of the labor laws. I have run through these in my testimony. I see our time is running short, but they run from 5,000 to 70,000 under OSHA, imprisonment of up to 6 months. The Family Medical Leave Act, Age Discrimination in Employment Act, all have no criminal penalties except for a $100 fine for failure to post penalties; the Fair Labor Standards Act, up to $10,000 and imprisonment of up to 6 months.

Now, these laws, I think everyone who can see, protect important rights, but Congress has seen fit to use civil and criminal penalties at a much lower scale than exists in the legislation before you; and again, I emphasize the degree of those penalties to dispel any notion that there is some weakness in this bill that would encourage noncompliance.

Contrary to what may seem to be a popular conception, many laws rely exclusively on government enforcement mechanisms and do not include private causes of action: Davis-Bacon Act, Service Contract Act, the Walsh-Healey Act, Executive Order 11246, 503 of the Rehabilitation Act, perhaps most notably the Occupational Safety and Health Act, the Mine Safety and Health Act and the National Labor Relations Act.

Now, of course, some of these statutes do include private causes of action, and in full disclosure, I am certainly not going to hide that fact; but in those cases, the remedies are limited typically to economic, out-of-pocket damages, and an atypical example is that of Title VII, the 1964 Civil Rights Act which, as many of you remember, was amended several years ago after 2 years and numerous hearings, much contentious debate, to include noneconomic damages capped at certain levels. However, it doesn't exemplify the situation we are here today facing because in that case you had 30 years of experience to go on which demonstrated that there was a problem. Here we are working on a clean slate.

Finally, I have listed through here many of the problems with private causes of action. There is a lot of studies referenced here. I will summarize them by saying they invariably conclude that about 50 percent of the money is lost to cure transactional costs, lawyers, other administrative costs, not plaintiffs and not defendants; and I cover that in three or four pages.

Now, I would like to close by saying, of course, there are those who would argue that a business need not fear litigation so long as it obeys the law. So a provision for a civil court litigation should only trouble those truly bad actors and not present a problem to others. The only problem with this argument is that it is patently false. The reality of laws in this country is that they are invariably complex and often simply vague with the lines of compliance uncertain and often changing. The Supreme Court handed down three decisions just a month ago on the Americans with Disabilities Act. No one knows when you are in compliance and when you are not. To expose employers to litigation, this sort of situation strikes us as just wrong.

In closing, our opposition to inclusion of a private right of action is premised on the straightforward notions that the civil and criminal penalties now in the legislation are quite severe and provide more than adequate deterrence; many laws are adequately enforced without private causes of actions; and three, lawsuits are a rough, blunt and expensive instrument of justice with many negative attributes which should only be used where there is a clear track record demonstrating the law in question currently has inadequate enforcement mechanisms, a record which certainly does not exist here. Should the Congress find that after passage of this legislation and a period of enforcement the business community is ignoring its responsibilities, it can always revisit the issue and authorize new enforcement mechanisms.

Thank you, Mr. Chairman.

[The prepared statement of Randel K. Johnson follows:]

PREPARED STATEMENT OF RANDEL K. JOHNSON, VICE PRESIDENT OF LABOR & EMPLOYEE BENEFITS, U.S. CHAMBER OF COMMERCE

Mr. Chairman and Members of the Committee, good morning. I am Randel Johnson, Vice President, Labor and Employee Benefits, U.S. Chamber of Commerce. The U.S. Chamber of Commerce is the world's largest business federation representing more than three million businesses and organizations of every size, sector and region.

Mr. Chairman, I have been asked to address the narrow issue of whether or not a private cause of action in court should be authorized under the legislation before you today, the "Medical Information and Research Enhancement Act of 1999." We believe the only reasonable answer to this question is "no" and the Chamber would strongly oppose inclusion of a new individual right to sue in addition to the severe civil and criminal penalties already in the legislation. Contrary to the assumptions of some, it is not true that a new right to sue must, or should be, created each time Congress creates a new substantive legal right or that such a right is necessary for effective enforcement. Furthermore, experience would suggest that—given the inherent negatives associated with court litigation—Congress reserve creation of new private causes of action in court for only those situations where there has been a demonstrated and well-documented problem with existing enforcement mechanisms. This threshold criteria has not been met here.

It should be emphasized that whatever is enacted will be an important, but complicated new federal law. Before we subject individuals and organizations to the expense and uncertainty of private litigation, we need to allow time for any uncertainties in the law to be clarified. Hopefully, much of this will be accomplished through administrative regulations that will flesh out the many rights, responsibilities and protections in the legislation, a far preferable course than the vagaries, expense and inconsistencies of the court system developing policy on a case by case basis.

Since the question of whether a private cause of action is necessary turns on whether or not the existing legislation has adequate provisions to deter violations of its provisions, we need to look carefully at what is in the legislation now. I urge the Members to refer to the actual text of the legislation in this regard because these existing sanctions are actually quite severe. First, let's review the criminal penalties under proposed Section 2801 "Wrongful Disclosure of Protected Health Information." Under this section, a "person that knowingly and intentionally" [1] discloses protected health information shall be fined up to $50,000, imprisoned not more than one year or both; and if the offense is committed under "false pretenses," be fined not more than $100,000, imprisoned up to five years or both. And if the offense is committed with "the intent to sell, transfer, or use protected health information for monetary gain or malicious harm" the person could be fined up to $250,000, and imprisoned not more than 10 years or both. All of these penalties and prison sentences could be doubled under certain circumstances. I also note that the "person" subject to these sanctions apparently could be anybody employed by, or

[1] We urge the committee to define this concept to encompass only knowing and intentional violations of the law in the sense that the individual knew his or her conduct violated the Act and intended harm.

with any connection to, the health information—from a clerical worker on up; hence the sweep of these provisions is quite broad.

Now let's turn to the civil penalties under new Section 311. Under this section, "a person" who the Secretary of Health and Human Services determines has "substantially and materially failed to comply with this Act" *shall* be subject to up to $500 for each violation and up to $5,000 for multiple violations arising from failure to comply with Title I of the act; and, where a violation relates to Title II, a civil penalty of up to $10,000 for each violation, and up to $50,000 in the aggregate for multiple violations, may be imposed. A $100,000 penalty is provided for violations which constitute a general business practice. This legislation also sets out detailed procedures for consideration of penalties under Section 312. The Secretary is empowered to seek injunctive relief.

To state the obvious, I can assure you that any entity covered by this legislation will take these civil and criminal penalties quite seriously, and I have to ask if there is anyone in this room today who would view these possible jail terms and monetary penalties lightly if they were subject to this law—I doubt it. I would ask you for one moment to put yourself in the place of an individual within a business handling health care information—of whatever size—and ask yourself that question.

To help demonstrate the extreme nature of these criminal and civil penalties, it might be useful to refer, for the purposes of comparison, to a few employment laws. Under the Occupational Safety and Health Act willful or repeat violations can be penalized by monetary penalties of between $5,000 and $70,000; a serious violation up to $7,000; a non-serious violation up to $7,000, and for failure to correct a violation, a civil penalty of not more than $7,000. With regard to criminal penalties, a willful violation causing an employee's death can be punished by a fine of not more than $10,000 and imprisonment for not more than 6 months or both, except that if the violation is committed after a prior conviction, punishment can be doubled.[2]

The Family and Medical Leave Act and Title VII of the 1964 Civil Rights Act contain no criminal penalties and only a civil fine of $100 for a willful failure to post a notice of FMLA and Title VII rights. The Age Discrimination in Employment Act has a criminal penalty of up to $500 or imprisonment of up to 1 year for interfering with an EEOC agent. Similarly, the National Labor Relations Act, protecting the rights of employees to unionize, provides only for a fine of not more than $5,000 or imprisonment for one year for interfering with a Board agent. The Fair Labor Standards Act contains fines of not more than $10,000 and imprisonment at up to 6 months for certain violations.

As you can see, the proposed civil and criminal penalties of the legislation before you are quite severe in comparison to other laws—laws which also protect important rights.

I led my testimony with a discussion on civil and criminal penalties to dispel any doubt that this legislation somehow provides an invitation for non-compliance or that such penalties are not otherwise adequate to deter violation. *Nothing could be further from the truth.* In this context, I turn to the question of the need for a private cause of action.

Contrary to what seems to be a popular conception, many laws rely exclusively on government enforcement for protection of important substantive rights, as does this legislation. In the labor area alone these include: The Davis Bacon Act (requires payment of prevailing wages on government contracts for construction), the Service Contract Act (requires payment of prevailing wages on government services contracts), the Walsh-Healey Act (payment of minimum wages and overtime to employees working on government contracts); Executive Order 11246 (prohibits discrimination by government contractors); Section 503 of the Rehabilitation Act (prohibits discrimination by government contractors on the basis of disability), and, perhaps most notably, the Occupational Safety and Health Act (protects employee safety and health), the Mine Safety and Health Act (protects safety and health of miners), and the National Labor Relations Act (protects the rights of employees to engage in concerted activities, including unionization.)[3]

Of course some labor statutes (in interest of full disclosure) do have a private cause of action, typically with remedies keyed to economic damages, such as lost pay with—in some instances—a doubling where the violation was willful or without good

---

[2] By operation of the 1984 Comprehensive Crime Control and Criminal Fine Collection Act, which standardized penalties and sentences for federal offenses, *willful* violations of the OSH Act resulting in a *loss of human life* are punishable by fines up to $250,000 for individuals and $500,000 for organizations.

[3] Other examples include the Paperwork Reduction Act, Section 17(a) of the Securities Exchange Act (see Touche Ross v. Redington, 442 U.S. 560 (1979)), and the Federal Service Labor Management Relations Act.

faith. (But let me again emphasize that these laws do *not* have the severe criminal and civil penalties contained in the privacy legislation.) An atypical example is Title VII of the 1964 Civil Rights Act, which was amended in 1991 to include non-economic damages (capped at various levels), but only after two years of much contentious debate encompassing two separate Congresses.

These changes were based on a long record of experience amassed over some 30 years, which demonstrated that by the 1990's changes were needed. Even with this lengthy consideration by Congress, the results have not been pretty. Litigation has exploded—tripling since 1991—with discrimination cases constituting almost one of every ten cases in federal court, the second highest number after prisoner petitions.[4] That only 5% of cases filed with the Equal Employment Opportunity Commission are found to have "reasonable cause" and 61% "no reasonable cause", tells us that many of these cases are of questionable validity. I've also attached for the Members' reference an article entitled, "Lawsuits Gone Wild," February 1998, discussing the plight of businesses under this surge of litigation. Litigation expenses alone to defend a case can approach $50,000—$150,000 even before trial.

Perhaps this isn't surprising given the nature of civil litigation, but it does emphasize the importance of Congress carefully deliberating before it authorizes individual civil litigation as a remedy. Indeed, the fact that private lawsuits are expensive, blunt enforcement instruments with enormous transactional costs can hardly be argued. While I do not wish to debate tort reform here, it may be worthwhile to refer to a few further facts on this issue:

A Tillinghast-Towers Perrin analysis (Nov. 1995) of the U.S. tort system found that when viewed as a method of compensating claimants, the U.S. tort system is highly inefficient, returning less than 50 cents on the dollar to the people it is designed to help—and less than 25 cents on the dollar to compensate for actual economic losses. (Tillinghast-Towers Perrin, "Tort Cost Trends: An International Perspective," pp. 4, 8)

The study broke down costs as follows:

Awards for economic loss 24%
Administration 24%
Awards for pain and suffering 22%
Claimants' attorney fees 16%
Defense costs 14%

Hence, even when non-economic "pain and suffering" awards are included, claimants ultimately collected only *46%* of the money raised, the balance going for the high transactional costs of the system.

These conclusions are consistent with a 1985 RAND study which indicated that plaintiffs in tort lawsuits in state and federal courts of general jurisdiction received only approximately half of the $29 billion to $36 billion spent in 1985. *The cost of litigation consumed the other half* with about 37% going to attorney's fees (pp. v—xi). A 1988 RAND study of wrongful discharge cases in California found that "total legal fees, including defense billings, sum to over $160,000 per case. The defense and plaintiff lawyer fees represent *more than half* of the money changing hands in this litigation." (pp. viii, 39-40) (The range of jury verdicts were from $7,000 to $8 million with an average of $646,855. pp. vii, 25-27, excluding defense judgements.) (Average award after post-trial settlement and appellate review was still $356,033, p. 36)

A March 1998 study by the Public Policy Institute entitled, "How Lawsuit Lottery is Distorting Justice and Costing New Yorkers Billions of Dollars a Year," applied the Tillinghast-Tower's analysis for New York's tort liability system and calculated that liability expenditures broke out as follows:

- $6.57 billion in payments to claimants (including $3.1 billion in pain and suffering awards and only $3.4 billion for actual economic damages).
- $3.4 billion for *administrative overhead.*
- *$2 billion for defense costs.*
- *And nearly $2.3 billion for plaintiffs' attorneys.*

The study found: "In sum, more than half of the money extracted from our consumers, our taxpayers, and our economy by New York's phenomenally expensive liability system doesn't go to its supposed beneficiaries" (p. 26).

---

[4] See study by Lawyers Committee on Civil Rights under Law, Daily Labor Report, March 25, 1999. The Americans with Disabilities Act includes the same remedies as Title VII although it was originally passed and enacted with only equitable relief. The ADA was premised on longstanding principles and regulations found under Section 504 of the 1973 Rehabilitation Act. Nevertheless, it, like Title VII since amended by the Civil Rights Act of 1991, has resulted in considerable litigation, much of it frivolous. See "Helping Employers Comply with the ADA," Report of the U.S. Commission on Civil Rights, September 1998, pp. 274-283.

And a May 1995 Hudson Briefing Paper, "The Case for Fundamental Tort Reform" noted that:

- The U.S. tort system needs to be made far more efficient and our society far less litigious and far larger shares of tort payments should go to injured parties rather than to lawyers. Currently, more than fifty cents of every dollar paid out of the tort system goes to cover attorneys' fees.
- Lawyers monopoly of access to the courts allows them to impose a 33.33 to 40 percent toll charge on all damage recoveries, even in cases in which defendants are willing to pay on a rapid no-dispute basis. Contingency fees, the near-uniform means of compensating tort claim attorneys, can provide risk free windfall profits to lawyers while harming defendants, plaintiffs, and the economy as a whole.

The real costs of the nation's tort civil litigation system is enormous[5], and the broader a civil action is in terms of grounds for liability and damages the more incentive there is for frivolous litigation—as many lawyers and plaintiffs seek to play the litigation lottery in front of juries for huge monetary rewards. However, my primary point here is that simple logic dictates that a system with such heavy transactional costs should, by definition, be considered as an option of last resort.

Of course, I realize that there are those who would argue that a business need not fear litigation so long as it obeys the law—so a provision for civil court litigation should only trouble truly bad actors and not present a problem to others. *The only problem with this argument is that it is patently false.* The reality of laws in this country is that they are invariably complex and, often, simply vague, with the lines of compliance uncertain and often changing. The Code of Federal Regulations governing the workplace arena alone covers over 4,000 pages of fine print, and hundreds of court and administrative decisions provide their own gloss of what the law is, or is not, on any given day. The Supreme Court handed down three decisions on the Americans with Disabilities Act just a month ago and two on what constitutes sexual harassment under Title VII and one on the Age Discrimination in Employment Act in the last session. Eleven Circuit Courts of Appeal render their own versions of the law. One treatise on discrimination law stretches over two volumes and two thousand pages of analysis with more footnotes, as does another on the National Labor Relations Act. And these are not atypical examples of one area of the law. Even enforcement agencies, with all their expertise, cannot give clear answers as to what is or is not required. (See "Workplace Regulation—Information on Selected Employer and Union Practices," GAO Report #94-138)

All of these problems are magnified when it comes to a new law, such as that before you today, which will, no matter how well drafted, be subject to much interpretation. Many times there will not be right or wrong answer and that problem will be heightened if courts across the country, likely combined with jury trials, are immediately faced with cases to sort out every nuance—which may very well differ from jurisdiction to jurisdiction—while the employer is faced with both uncertain requirements and liability.

In closing, our opposition to inclusion of a private right of action is premised on the straightforward notions that (1) the civil and criminal penalties now in the legislation are quite severe and provide more than adequate deterrence, (2) many laws are adequately enforced without private causes of actions, and (3) law suits are a rough, blunt and expensive instrument of justice with many negative attributes which should only be used where there is a clear track record demonstrating that the law in question currently has inadequate enforcement mechanisms—a record which certainly does not exist here. Should the Congress find that, after passage of this legislation and a period of enforcement, the business community is ignoring its responsibilities, it can always revisit the issue and authorize new enforcement mechanisms.

Thank you.

Mr. NORWOOD. Thank you, Mr. Johnson, and I will ask all of you to excuse us for a few minutes. We have a few votes, and we all want to hear you. We will go into recess, and I will ask you to stay very close by because we will all be back just as quickly as we can.

[Brief recess.]

[5] For other overviews of expenses associated with court litigation, see, generally, *The Illinois Tort Reform Act: Illinois' Landmark Tort Reform: The Sponsor's Explanation,* 27 Loy. University of Chicago L. J. 805, Summer 1996. Also see *Symposium: Municipal Liability: The Impact of Litigation on Municipalities: Total Cost, Driving Factors, and Cost Containment Mechanisms; 44 Syracuse Law Review 833, 1993.*

Mr. GREENWOOD [presiding]. Welcome back. I am told that in my absence Ms. Carty and Mr. Johnson have testified and we are ready to hear from Dr. Andrews; is that correct?

In that case, if you will please proceed.

STATEMENT OF ELIZABETH B. ANDREWS

Ms. ANDREWS. Thank you. Mr. Chairman and members of the committee, my name is Elizabeth Andrews, and I am Director of Worldwide Epidemiology at Glaxo Wellcome, a research-based pharmaceutical company that is based in Research Triangle Park, North Carolina.

Glaxo Wellcome is committed to the enactment of Federal legislation that would protect patients' confidentiality while assuring the availability of medical information for research and for the delivery of quality health care. For this reason, we strongly support Congressman Greenwood's H.R. 2470, the Medical Information Protection and Research Enhancement Act of 1999, because we believe this legislation best meets that goal.

Today, medical researchers are poised to make countless new discoveries that will alleviate the burden of disease. That promise will only be realized, however, if medical researchers are allowed to continue to have access to patient medical information for research. Both interventional research, involving collection of information directly from individuals, such as in a clinical trial, and observational research, the analysis of existing medical records without contact with or impact on individuals, rely on the use of individually identifiable medical data. Not all research can be conducted using strictly anonymized records. Federal legislation must facilitate the positive uses of medical information if we are to continue making breakthrough scientific achievements into the future. The Greenwood bill provides a strong, promising framework to do so.

The Greenwood bill would also establish uniform national standards for organizations that manage health data, including research institutions, to assure they have strong safeguards and internal procedures for protecting that data. Moreover, the bill would impose penalties on institutions that fail to adopt or enforce the safeguards.

A recent GAO study on the use of medical data and research concluded that safeguards already exist in many organizations conducting research outside the Federal system. In fact, the GAO's findings are consistent with the widespread belief in the research community that researchers are doing a thorough job of protecting the confidentiality of patients while conducting research with extremely valuable public health benefit.

We also hope that new legislative requirements will complement existing research regulation without needlessly complicating it. We are opposed to expanding the scope of the Federal common rule and the approval of institutional review boards to all public and private research, even research using only observational existing information as required in some legislative proposals.

IRBs play a valuable role in carrying out their mandate to ensure that research participants are fully informed of the risks they incur when undergoing experimental medical treatment. However, IRBs have neither the expertise nor capacity to review research

proposals, and to review studies with respect to confidentiality practices. Requiring IRB review of all research in this country would threaten the system that is already overburdened. Expanding IRB review would needlessly complicate the important tasks already faced by IRBs and would harm research by subjecting each project, each hypothesis to burdensome review and consent requirements. The likely result would be that many important research projects would never be initiated.

In Glaxo Wellcome's view, the process established by the Greenwood bill is more protective of patient confidentiality interests than the expansion of IRB review and informed consent requirements. Enforceable, uniform national standards for confidentiality protections would offer more appropriate, more consistent and more rigorous controls than available through an expansion of the IRB function.

With respect to patient consent, we support current Federal requirements concerning the informed consent of participants in interventional research. We do not believe, however, that observational research programs using archives of previously collected information should require informed consent. In many cases, it is impossible to gain consent. Patients move, they change health plans, they die, and given the extremely minimal risk for patients from this type of research, requiring informed consent increases the burden on researchers and patients, but does not serve to protect the patient's confidentiality interests. Furthermore, allowing patients to opt out of observational medical records research would raise serious questions about the scientific validity of conclusions reached from incomplete data bases.

One critically important issue for any confidentiality legislation is that it must draw clear distinctions between protected health information and nonidentifiable information. The Markey and Condit bills define protected health information so broadly that almost no information could be characterized as nonidentifiable. As a result, every piece of health care data, whether or not it identifies an individual, would be subject to all of the Federal restrictions and requirements applicable under the law, including written consent, recordkeeping, access to copying and amendment notification.

Mr. Chairman, members of the committee, we urge you to take swift action on the Greenwood bill to ensure that Congress meets its HIPPA deadline of August 21st, rather than allowing the Secretary of Health and Human Services to promulgate regulations in this area. Patients, health care providers and researchers have much to lose if legislators do not strike a balance between protection of patient confidentiality and the appropriate use of medical data to enhance the quality of health care delivery in this country.

I look forward to working with you as you continue your efforts and stand ready to help the committee in any way. Thank you.

[The prepared statement of Elizabeth B. Andrews follows:]

PREPARED STATEMENT OF ELIZABETH B. ANDREWS, DIRECTOR, WORLDWIDE EPIDEMIOLOGY, GLAXO WELLCOME INC.

Introduction

Mr. Chairman and Members of the Committee, my name is Elizabeth Andrews, and I am Director of World Wide Epidemiology for Glaxo Wellcome, a leading research-based pharmaceutical company. This year, Glaxo Wellcome will spend nearly

$2 billion on research of new medicines for the treatment of cancer, diabetes, obesity, rheumatoid arthritis, osteoporosis and viral diseases. As an industry, the nation's research-based pharmaceutical and biotechnology companies discover and develop the majority of new medicines used in the United States and around the world, investing more than $24 billion this year alone on research and development. The industry brought 39 new prescription drugs and biologics to market last year to treat many deadly and debilitating diseases.

Medical Information is Essential for Research

Mr. Chairman, I would like to begin by thanking you for the opportunity to testify this morning on behalf of Glaxo Wellcome on the important issue of federal legislation to protect the confidentiality of medical information. As a scientist whose work is committed to discovering and improving health care interventions, I am pleased that this Committee— which has responsibility for legislation affecting American health and health care— will play a leading role in crafting that legislation. I look forward to working with you.

Glaxo Wellcome strongly supports new federal legislation that would protect the confidentiality of individuals' medical records from unauthorized or inappropriate use. At the same time, we know that appropriate use of medical information is critical to the delivery of high quality health care and the development of innovative and more effective treatments for patients. We hope that the committee will pass legislation that will result in enactment of a new federal law that safeguards patients' medical privacy while allowing appropriate uses of medical information for research, treatment, payment for services and health care operations. We feel that legislation introduced by Congressman Jim Greenwood, H.R. 2470, "The Medical Information Protection and Research Enhancement Act of 1999," achieves that balance. Glaxo Wellcome strongly supports H.R. 2470, as well as similar legislation, S. 881, introduced by Senator Robert Bennett. We urge the Congress to take action on these bills to meet the August 21, 1999 deadline established by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to enact a medical data confidentiality law.

The pharmaceutical and biotechnology industry can help patients with unmet medical needs only if researchers have access to medical information that enables them to discover new medicines. Today, medical researchers are poised to make countless new discoveries that will alleviate human suffering and the burden of disease. Revolutionary new treatments and diagnostic tests promise to extend and enrich our lives and the lives of future generations. Realizing this promise depends on research: interventional research involving the collection of information directly from individuals such as clinical trials used to develop new drugs, medical devices and biologics; and observational research which relies on existing databases. Observational research allows us to study of the prevalence of disease, evaluate medical treatments and measure the cost-effectiveness of therapies. Observational research can sometimes be conducted with encoded or encrypted data that has been stripped of individual indentifiers, while preserving the ability to link various databases across treatment settings and over the course of time to capture a comprehensive picture of patient care. Having the complete picture of the patient's health and health care is what is essential for the researcher, not the identity of the patient.

As an epidemiologist, I would like to provide to the Committee some examples of research that will explain how we use medical information to help improve the health of patients and the quality of health care delivered to them. I have been involved in the study of HIV/AIDS and other sexually transmitted diseases, the medicines developed for such conditions, and the risk of medicines when used in pregnancy. In these areas, we have made significant strides, coupling drug development programs with company-sponsored public health monitoring activities.

Through such efforts, we ensure the safe use of products developed to treat many serious diseases. There is increasing public attention given to drug safety monitoring and a need to assess the current mechanisms available to evaluate the safety of medicines. Most health professionals agree we need more, not less, information on the safety of medicines in order to better understand the risks compared to the benefits of drugs as they are used in general, not experimental, circumstances. It is through the use of archival medical records that we are able to understand such risks and benefits in large numbers of patients in the real world setting. Each of the following examples involves research using archived medical information.

- An epidemiologic study in the early 1980s that found a strong association between the potentially fatal Reye's syndrome and children's use of aspirin. Eventually, this new knowledge led to a decline in cases of Reye's syndrome in the United States, improving children's health and reducing mortality.

- A recent study documented both the under-use of beta-blockers following myocardial infarction in the elderly, and the serious consequences of that under-use. This study linked large pharmacy and medical claims databases. Its finding of unnecessary deaths and hospitalizations from cardiovascular episodes is likely to lead to basic changes in medical practice and greatly improve patient health.
- A pharmaceutical company worked with a large managed health-care plan to undertake a study of more than 85,000 children to provide further information on the safety of the chicken pox vaccine in clinical practice. These children received the vaccine, with parental consent, as part of their regular medical care. A computer-based search was performed of the records of the children who received the vaccine and of a historical comparison group of children who had not used the vaccine. The medical records of the children who had not been vaccinated were taken from the plan's historical archives of patient records. It would have been extremely difficult, if not impossible, for the health plan to track them down to gain their consent. The information received by the pharmaceutical company was encrypted, so that the company had no patient-identifiable data. This research has provided valuable reassurance about vaccine safety under conditions of broad use in clinical practice.
- A health plan was able to use medical information about its enrollees to identify women with a deficient gene that is linked to some breast cancers. The health plan contacted these women, many of whom chose to enroll in the federally-regulated and IRB-overseen clinical trial that a pharmaceutical company conducted of a new drug to treat breast cancer. Had the health plan been unable to review these women's records and contact them, there would have been significant delays in finding appropriate participants for the clinical trial.

Because of the focused and controlled nature of clinical trials, much of what we learn about drug safety and effectiveness is learned through the use of observational data after drug approval. In the area of HIV, for example, we learned from observational experience that differences in HIV disease progression seen by gender, race and intravenous drug use were not due to those patient characteristics, but due to differences in treatment and access to treatment. Observational studies demonstrated the effectiveness of pneumocystis carinii pneumonia (PCP) prophylaxis, and quantified the adverse experience rates with antiretroviral therapies and various treatments for opportunistic infections. All of these findings have contributed to more effective care and better outcomes for patients with HIV.

In addition to ongoing safety surveillance studies, health care payers in our cost-conscious system demand more focused outcomes research and economic analysis to select the most efficacious and cost-effective treatment options. For example, Harvard Medical School researchers found that restrictions on the use of schizophrenia medications in the New Hampshire Medicaid program proved penny-wise but pound-foolish. The restrictions yielded some savings on prescription drugs, but ultimately increased state and federal government Medicaid spending overall by sharply increasing the need for emergency care and hospitalization. The Harvard team produced these findings—which can promote both better health care for patients and more cost-effective use of health care dollars—by linking prescription drug use databases with mental health center and hospital data.

These examples illustrate the useful and important observational research that is being conducted with existing medical records, while using various methods for safeguarding the confidentiality of patients. These methods include replacing individual identifiers with a case code number and safeguarding the key from unauthorized use or disclosure, restricting the subset of persons who have access to research databases, and ensuring that employees are aware of their obligation to treat research data as confidential and to protect it from disclosure and unauthorized use.

Medical Data Confidentiality Legislation

Glaxo Wellcome believes that the Greenwood bill, H.R. 2470, provides a workable framework for protecting patient health information while also recognizing the need to access patient data for legitimate health care-related purposes—primarily treatment, payment, health care operations and medical research. It establishes very clear boundaries around the permissible uses and disclosures of patient medical data and imposes strong penalties on entities and individuals for its misuse.

We feel that strong federal confidentiality protections must complement existing research regulation without needlessly complicating it. For that reason, we are very concerned that H.R. 1941, introduced by Congressman Gary Condit, as well as H.R. 1057, introduced by Congressman Edward Markey, would extend Institutional Review Board (IRB) and informed consent requirements to all private research that has traditionally not been subject to the federal common rule.

Informed consent, which is a cornerstone of the interventional research that is reviewed by IRBs, does not work in the context of database research. In database research, the validity of the scientific conclusions depends on how comprehensive the database is. The researcher does not affect the treatment of the individuals, rather he or she tries to make inferences based on observed differences in ordinary health care settings. The validity of those inferences is suspect if the researcher is missing information from some individuals. What we know based on the experience in Minnesota, which has a law that requires informed consent for medical records research, is that individuals who decline to give consent are not a random sample. This means that imposing informed consent requirements on research databases has the effect of undermining the generality and validity of the conclusions that can be drawn based on research using that database.

Moreover, a recent General Accounting Office (GAO) report examined the protection of patient medical data used in medical research. We were encouraged that GAO's findings are consistent with the widespread belief in the research community that researchers are doing a thorough job of protecting the confidentiality of patients while using medical information in extremely important research concerning public health and health care delivery. The GAO report makes some important points which accurately reflect the current status of research conducted outside the federal system.

First, the report acknowledges many uses of information and data in research, and provides examples of important research that required some type of access to identifiable information. Not all research can be conducted strictly using anonymized records. Research based on archival records with no medical risk to the patients and rigorous safeguards of personally identifiable data should be encouraged, not impeded.

Second, the report provided examples of a variety of safeguards that are in place in different types of organizations that undertake research outside the federal system. The examples demonstrate clearly that many safeguards already exist to protect the confidentiality of identifiable patient information. Those safeguards are tailored to the local needs and circumstances within each organization. Institutions conducting health research take confidentiality of patient information very seriously. The report aptly notes that the institutions in their study may not represent all organizations, and those not studied may not meet the same high standards of those in the study. However, the Greenwood bill would establish uniform national standards that would be required for all organizations that manage health data. Moreover, it would provide for penalties for organizations that fail to adopt or enforce the safeguards.

Third, the report provided a realistic picture of current IRB operations. IRBs provide a valuable function in protecting patients from unnecessary research risks. Their experience and expertise in reviewing studies only for review of confidentiality practices is insufficient to warrant such an expansion of their roles. Moreover, they do not have the capacity to handle the increased volume that would emerge from a new requirement to review all medical records research. We feel it would be counter-productive to institute such a requirement. Uniform national standards for confidentiality protections would offer a more appropriate, more consistent, and more rigorous controls than available through an expansion of the IRB function.

In Glaxo Wellcome's view, the process established by the Greenwood bill is *more* protective of patient confidentiality interests than the expansion of IRB review and informed consent requirements that would be put in place under H.R. 1941 and H.R. 1057. For instead of needlessly complicating the important tasks already faced by IRBs, the Greenwood bill would provide federal enforcement of the safeguards and review process established by each research institution. In this regard we note that GAO reports that even where they do review projects, IRBs say they rely on the practices and safeguards in effect at the research institution. This fact is important, because to truly understand and oversee what an institution does to protect the confidentiality of data is far beyond what an IRB can or should be charged with doing in its review of a research project. The Greenwood bill would ensure that what GAO found to be true of the institutions it surveyed— they have policies and safeguards designed to protect confidentiality— would be enforceable as a matter of federal law. The bill would provide the further assurance that every institution making medical information available for research would be required to establish such federally enforceable policies and safeguards.

I would like to summarize for the committee the key issues that we have identified in previous legislation that could create impediments to our continuing ability to conduct medical research:

- *Definitions.* It is critically important that any confidentiality legislation draw clear distinctions between "protected health information" and "non-identifiable" infor-

mation. Both H.R. 1917 and H.R. 1057 define protected health information so broadly that almost no information could be characterized as "non-identifiable." As a result, many vital activities, including research, that rely on non-identifiable information would be subject to burdensome prior authorization requirements.

- *IRB oversight of research.* Pharmaceutical and biotechnology companies comply with IRB requirements when sponsoring clinical trials in support of new drug or biologic and we believe that IRBs effectively protect the welfare of trial participants. As noted above, we do not believe that IRB oversight should be extended to every analysis of medical information or to research that is not federally regulated, sponsored or funded, or modified to encompass unique confidentiality issues.
- *Patient consent.* We support current federal requirements concerning the informed consent of participants in interventional research. We do not believe, however, that research projects using databases or archives of previously collected information and materials should require informed consent. In many cases, it may be impossible to gain consent—patients move, change health plans, die—and given the extremely minimal risk to patients from research of this type, requiring informed consent increases the burden on researchers but does not serve to protect the patient's confidentiality interests.
- *Retention of data.* Researchers should not be required to destroy data once the original study for which it has been collected has concluded. In some cases, it is necessary to retain the data in order to comply with existing federal regulations. In other cases, the collected data can be extremely valuable and may be reanalyzed for other purposes beyond the original intent and would be beneficial to patients.
- *Provide Uniform, National Protection for All Medical Information.* The same confidentiality standards for all types of medical information should apply nationwide. Legislative distinctions among types of medical information— genetic, psychological, or physical— would conflict with the patient's expectation that all health care information shared with a provider to obtain appropriate treatment should be maintained in confidence. Further, to ensure that individuals' expectations of confidentiality of medical information are valid in every jurisdiction, federal law should provide a uniform set of national requirements that would preempt state laws.
- *Penalties.* Finally, Glaxo Wellcome supports strong penalties for violations of patients' confidentiality that have been included in most of the legislative drafts. We do not believe, however, that these penalties could or should include enforcement tools such as exclusion from the Medicare and Medicaid programs. We believe that strong penalties, including civil monetary penalties, are a more effective deterrent to misuse and a more appropriate punishment for violators.

Principles for Protecting Patient Confidentiality

As is the case with other companies, Glaxo Wellcome is an active member of the Pharmaceutical Research and Manufacturers of America (PhRMA), the Biotechnology Industry Organization (BIO) and the Healthcare Leadership Council (HLC). We have been working closely with these organizations and other members of the health care provider community on this important issue. We were particularly involved in PhRMA's efforts to develop a key set of principles that reflect a commitment to strong protections for individuals' medical information while ensuring the availability of medical information for research and for the delivery of quality health care. A copy of these principles is attached.

Conclusion

Mr. Chairman, Members of the Committee, I again wish to express Glaxo Wellcome's appreciation for your efforts and your obvious attention to protecting the public's interest in the fruits of health research. We look forward to working with you as you continue your efforts, and we stand ready to help the committee in any way.

Mr. GREENWOOD. Thank you very much, Dr. Andrews, for your testimony.

Dr. Koski.

STATEMENT OF GREG KOSKI

Mr. KOSKI. Thank you very much, Mr. Chairman and members of the committee. My name is Greg Koski, and I am the Director

of Human Research Affairs for the Partners Health Care System in Boston.

In both my professional and personal life, I have had an opportunity to consider very directly many of the issues we are talking about today, both as a doctor and as a patient, as a scientist, as well as a research subject. I also work as a manager, serve on the committees that are charged with formulating the confidentiality guidelines and policies and procedures. I have also served for more than 15 years as a member and chair of the IRB, and in my present capacity, am responsible for the overall protection of human subjects in research for our entire large integrated health care system.

In today's hearing, we have heard the words "privacy" and "confidentiality" used frequently and often interchangeably, and I think for the sake of clarity it is worth expanding on that just a bit little bit. Clearly, the right to privacy is the right that an individual has to actually choose the extent to which they wish to share information about themselves and their activities with other individuals, and when in the course of their social activities and interchanges they make the decision to share that information, they are allowing the open door into their world of privacy, but in doing so, they establish a centralist part of the social contract or confidentiality agreement, the extent to which and the expectations according to which that information is being shared.

Whenever we try to access private information without appropriate authorization or where we have no right to that information we are clearly invading privacy. When we have been given private information under certain expectation of confidentiality and have failed to uphold it, we have breached confidentiality. Both of those are egregious, and I believe should have appropriate penalties associated with them.

But I think if we look at this realistically, it would simply be impossible in our modern age to expect absolute privacy in any aspect of our lives. Certainly the health care system is no exception to that, and in fact, it is absolutely essential in seeking care and in managing care that individual privacy be compromised to a certain degree or there are risks on both sides, both to the individuals as well as to society and the institutions.

So I think that it is clear from the discussion that we have had today, that I won't reiterate, that we have reached a situation where we have begun to lose public confidence in our ability to protect them and their private health information; and I believe that now is the time to take steps to try and establish appropriate procedures, policies, laws for the necessary protections.

A few points that I would emphasize as being essential toward this goal would be, in no particular order, that we actually collect only that information that we truly need, that is justified for what we need to do. By not having information that you don't want, the risks that something might be done with it that is not appropriate are greatly alleviated.

Similarly, information that is collected for one purpose should be used for that purpose or that set of purposes and should not be used for secondary purposes without some appropriate degree of oversight and authorization. At times, that will be from the individ-

ual, at times it will be from another body, but that depends upon the nature of the risks involved and sensitivity of the information.

Overall access to personal health information should be strictly available, limited on a need-to-know basis rather than a want-to-know basis.

Unauthorized uses of information should be subject to appropriate penalties and clearly any entity or entities that are actually collecting or receiving personal health information should do so under appropriate policies and only with appropriate policies for properly protecting the confidentiality.

Clearly, confidentiality in itself is the process that we use to demonstrate our respect for the privacy of individuals, and when we accept private information, we also accept that moral and legal obligation to ensure that we carry out the confidentiality process in a robust manner.

When an institution produces or publishes its policies for confidentiality, I think it is essential that those be shared in a very active and informed way with the individuals whose information is going to be accessed.

And finally, these policies should include specific provisions that would minimize risk of any disclosure by, to the fullest extent practicable, using nonidentifiable information when it can be used, using deidentified information, when appropriate, and only relying upon identifiable information as necessary.

I think I have a major exception to the language describing nonidentifiable in Mr. Greenwood's bill, and we may come back to that later on, but I want to turn my attention specifically to the issues of research.

In this country, biomedical research is conducted according to a variety of codes of ethics and all, the Nuremberg Code, the Declaration of Helsinki and certainly the Belmont Report, and three fundamental principles have been identified: respect for persons, justice and beneficence. All three of those fundamental principles for the conduct of research require that we respect the privacy of individuals who are participating in research and that we protect their confidentiality.

As a consequence of this and the incorporation of those fundamental principles into the laws, the common rule as it is called, or 45 CFR 46, as amended, all federally funded research is currently conducted in a manner that is consistent with those ethical policies; and indeed IRBs that are responsible for review and approval of all research involving human subjects under this Federal law are obligated to consider not only medical risks, but also psychological, social, economic risks as part of their considerations in determining whether or not the research should go forward.

With all due respect to Dr. Andrews, I think that it is very misleading to suggest that IRBs are neither in possession of the expertise or experience to do this because, in fact, it is inherent in what they do in the conduct of their business every day.

Large institutions with significant Federal funding, like our own, operate under an assurance to the Federal Government that we will apply the principles of the laws on the common rule to all research that is conducted at our institutions regardless of the source of funding; and unfortunately, only about 1,200 of the more or less

5,000 IRBs that currently review research in this country come under that common rule, and I think that is a glaring deficiency.

I think it is important to note that a common rule specifies when it talks about the definition of human subjects research not only the use of living human beings, but also information or specimens derived from living human beings. No one could misconstrue that to believe that the IRBs are not supposed to be reviewing research that involves identifiable patient information and to grant exemptions in the case where information has been rendered nonidentifiable.

Mr. BILIRAKIS. Please summarize, Doctor.

Mr. KOSKI. Thank you. I will.

I think what we should do at this opportunity—rather than to establish, as 2470 and 1941 would do, a parallel and probably unequal process for review of a subset of human research in this country, what we should do would be to take this opportunity, as the Secretary seems to be doing presently in the elevation of OPRR from NIH to a higher status at DHHS, to actually bring all human research under a common set of guidelines. I believe that this would be the highest and most appropriate way to actually ensure the protection of human subjects in research. There are opportunities to work with industry to define the mechanisms by which we can most effectively use deidentified information to meet their needs and at the same time respect the privacy of our patients.

I will stop there and hope to expand on some of that during our discussion.

[The prepared statement of Greg Koski follows:]

PREPARED STATEMENT OF GREG KOSKI, ASSOCIATE PROFESSOR OF ANESTHESIA AND CRITICAL CARE MEDICINE, MASSACHUSETTS GENERAL HOSPITAL

Dear Mr. Chairman and Members of the Subcommittee: Few would argue that individuals in this country reasonably expect that their privacy be respected, and that sensitive personal information about themselves, whatever the nature of that information might be, should not be disclosed to others without authorization, except in specific circumstances where there is a compelling need, and even then, only with specific provisions for protecting confidentiality of such information. Health information is arguably among the most sensitive types of personal information and has always been afforded special consideration when issues of privacy and confidentiality are concerned.

The extraordinary scope of social and technological change in our health care system over the past two decades has unavoidably and irrevocably changed the practice of medicine and the business of health care. With this change, the public has become increasingly concerned about the loss of autonomy and loss of privacy, both of which seem now to occur too frequently. Concerns regarding unauthorized access to personal medical information arise from, and are substantiated by, misuse and even abuse of information obtained during encounters with the health care system. A climate of mistrust has developed in which patients are demanding more control over who has access to their personal information and how that information is to be used. Since many do not understand the complexity of our health care system and the growing need for many different parties to access patient information in the course of their jobs, the adverse impact that broad restriction of access can have on the system, and the quality of care, is not well appreciated.

Several detailed and thoughtful analyses and reports have been presented addressing the complex issues involved in providing and managing health care while respecting the privacy of individual persons and protecting the confidentiality of personal health information. Current legislative activity pertaining to these issues at both the state and national levels reflects to a large degree the growing interest among our citizens and the entire health care system and related industries in finding effective ways to achieve these goals. One such effort is that of the Health Privacy Working Group, an initiative of the Georgetown University Institute of Health

Care Research, which recently released its recommendations. These include a set of "best principles" that provide a useful framework for development of specific policies for effective management and use of personal health care information in a manner that is well-reasoned and workable. The members of the Subcommittee will certainly receive copies of this report and will find it informative and useful. This statement of principles does not, however, obviate the need for effective legislation to affect necessary change and introduce appropriate safeguards for protection of privacy and confidentiality of health information.

Several pieces of legislation are currently under consideration by Congress, and the Secretary of the Department of Human Services has introduced a comprehensive set of recommendations as required by law that may take effect if Congress does not itself take action. Regardless of what legislation may ultimately be enacted, it should include a requirement that all persons, institutions, agencies or other entities which collect personal health care information be required to develop formal written policies and procedures for use of such information, and that patients be notified and informed of these policies and their rights.

These policies and procedures should limit access and distribution of information on a rigorous "need to know" basis. Information should only be collected and maintained in identifiable form when necessary and appropriate, it should be used only for those specific purposes for which it was intended at the time of collection unless there is appropriate notification and authorization of other uses, and when information is no longer needed, it should be destroyed or rendered nonidentifiable after a reasonable period of time unless there is a compelling justification for keeping it. If these general guidelines are kept in mind, mistrust and misuse of such information will be minimized.

I would like to thank Mr. Bilirakis and the members of the Subcommittee for this opportunity to offer general comments about the bill currently before it, H.R. 2470, otherwise known as the "Greenwood Bill". Those who have crafted this proposed legislation deserve a great deal of credit for their thoughtful work, as many of its provisions could provide useful solutions to some of the concerns discussed above. Nevertheless, there are aspects of this bill that could be improved. I will first offer a few remarks regarding the broader aspects of the proposed legislation before focusing on those parts of the bill pertaining to appropriate conduct and oversight of health research, an area in which I can claim some experience.

First, for clarity, I would like to call your attention to the definition of "nonidentifiable" health information used in this bill. Personal health information that *can* be attributed to the individual person from whom it was obtained is identifiable. Only information that *cannot* be attributed to its source is nonidentifiable. When information is linked by a specific code number to an individual, even if all other specific identifying information has been removed, that information is still identifiable and special precautions must be taken to restrict the use of that information in ways that have not been authorized by the individual of origin. The use of this term in the proposed legislation contradicts the definition set forth in the Federal Regulations for Protection of Human Subjects in research, is confusing and misleading, and will be viewed by many as being deceptive, intended or not. Information is either identifiable or not; these are mutually exclusive. Identifiable information may be anonymous, encrypted, coded, or deidentified in an effort to offer protection of privacy and ensure confidentiality, but it is still identifiable.

The description of "health care operations" is useful, but the list includes certain activities, such as outcome assessments, that frequently overlap the research domain, which I will discuss in greater detail below. Care should be taken to insure that this does not provide a "loop hole" for individuals to circumvent review and approval processes of Institutional Review Boards (IRBs) and the protections such review can provide.

The bill includes provisions for disclosure of information to a variety of third parties for a variety of purposes. As a general rule, any and all releases of identifiable health information to third parties outside of the health care setting in which it was obtained should be authorized by the individuals from whom the information is obtained. Secondary "re-disclosure" to parties further removed from the primary source/custodian should be prohibited and punishable by law.

While there is clearly a need to establish a minimum standard under federal law for protections of privacy and confidentiality of personal health information, a preemptive law that would undermine or limit the ability of States choosing to pass more stringent protective laws may have a counter-productive effect, actually reducing protections for individuals. Indeed, some may view such an attempt to preempt legislation at the State level with skepticism and as an attempt to protect special interests that may be in conflict with those of individuals.

Turning to the provisions for access to personal health information for research, I would first point out that the benefits of biomedical research to both society and individuals is widely acknowledged and very highly valued by the American people. In a recent national survey, nearly 90% of those polled indicated strong or very strong support for biomedical research activities and a personal interest in participating in research, *provided they could be assured that their interests and well-being were protected.* There is a long and very productive tradition of using medical records and other forms of health information for research purposes in this country, and such uses have rarely resulted in breaches of confidentiality. The American people have been very willing to accept this exception to absolute *privacy* of their medical information, provided the information is handled in a *confidential* manner.

We are very fortunate to have in place in this country a system for protection of human subjects in research, including federal laws that mandate oversight of research by duly constituted Institutional Review Boards. This system, in which I am a proud and active participant, already reviews and approves most of the biomedical research conducted in this country, including research that relies upon the uses of personal health information. The challenges faced by the IRBs are considerable, but overall, it is clear that since the IRB system was developed two decades ago, biomedical research involving human subjects has flourished and reports or serious abuses are infrequent. Even as this Subcommittee considers legislation to enhance protections for patients' privacy and confidentiality of health information, steps are being taken to strengthen the IRB system to make it even more effective. I strongly support these actions, and believe that the IRB process can and should play an integral role in oversight of all research involving health information.

I further support current efforts to bring all research involving human subjects, as defined in federal regulations, under the "Common Rule" (45 CFR 46, as amended), and to develop a process to credential IRBs and health researchers as a further step toward strengthening the system for protection of human research subjects. While existing rules and regulations offer the IRBs and investigators guidance in the use of personal health information, more specific guidance should be promulgated to address issues of informed consent, uses of identifiable versus nonidentifiable information, and specific mechanisms for protection of confidentiality. In some cases, it may be appropriate for institutional "confidentiality committees" to oversee access to personal health information at institutions that do not have sufficient research volume to justify an IRB, but even in those cases, the research should be reviewed and approved by an IRB constituted under the "Common Rule" according to specific guidelines for research access.

In large institutions and in the growing number of integrated health care systems, of which the Partners HealthCare System is an example, the co-existence and close association of such confidentiality committees and IRBs afford completeness and consistency in policies and procedures for access to personal health information that, at least in our case, has proven to be very beneficial. As information technology and electronic medical records systems play an ever growing and important role in modern health care and research, every practicable effort should be made to take advantage of new tools and methodologies of information science to enhance protection of sensitive information and patient privacy.

In closing, I would like to thank all of the members of the Subcommittee for the opportunity to express these views. I wish you all well as you address the challenges that lie ahead.

Mr. BILIRAKIS. Thank you, Doctor.

Dr. Frey.

STATEMENT OF CAROLIN M. FREY

Ms. FREY. Mr. Chairman and members of the committee, I am Carolin Frey, Chair of the Institutional Research Review Board for the Geisinger Medical Center, part of a larger health system and managed care organization. I appreciate the opportunity to speak to you today, specifically about the current role of the Institutional Review Board, or IRB, in protecting privacy as it relates to research.

Our IRB, like others, has witnessed growth in research made possible by large pools of extant and identifiable medical information. We have taken a proactive role in setting standards for con-

ducting this type of research. We do this in part because the IRB function has a lot to do with engendering public trust. To that end, the IRB's function is a valuable model, and I stress "model" with respect to pending privacy legislation, the IRB function is exactly that, a model and not a ready-to-use resource. The current IRB system works well in the places it has been implemented, but it does not provide universal oversight for research. Legislation must distinguish between the existing IRB infrastructure and an IRB-like process that could be designed.

I will now identify two limitations to the existing IRB function which would need to be overcome in legislating a process for universal review of research involving personal medical information, should that be a goal.

Now, first, the existing IRB system was never designed to provide universal protections. Not all institutions conducting human research have an IRB and not all IRBs review the special class of research involving extant and identifiable medical information. Institutions constitute IRBs usually because they are federally funded for human research or have investigations of FDA-regulated products being conducted there. However, these same institutions, such as Dr. Koski's and my own, may decide to apply the Federal regulations to all of their research. Some may choose to apply it to some.

Also, when identifiable medical information travels between institutions, one with and one without an IRB, it is possible for only a portion of an individual's record to be within the purview of an IRB. Complete, not partial, protection should be the goal of national legislation.

So let me now propose adequate protections that an IRB-like system would include: first, an orderly process for defining the purview of responsible reviewing entities to ensure complete and nonoverlapping protection; and second, be mandated at a sufficiently high Federal level to ensure a review board is available to all locations where this kind of research takes place.

Now, a second limitation of the IRB role concerns the fact that its role in protecting privacy is not well understood by the public. Where an IRB is used its strength is its authority to require strong security measures, sometimes likened to a firewall, to protect the privacy of identifiable medical information used in research. However, the specific review procedures used, including exempting review altogether, the conditions necessary to waive consent but also the societal benefits of such research are not well understood.

The IRB function broadly provides protection of human subjects from physical, social, mental, privacy and confidentiality risks. Use of extant personal medical information is just one special class of research. An IRB may, in fact, exempt from review that information which is essentially anonymized, but with recorded identifiers, this class of research generally qualifies for an expedited review carried out by a single IRB member.

It is important to point out that expedited IRB review does not by itself result in an exception to the requirement to obtain the individual's consent. First consideration is given to whether the merit of the proposed research warrants an intrusion, and that potential risk relies to some extent on the data security procedures proposed.

These protect against subsequent disclosures which are, in fact, the primary risk of this type of research.

An IRB can impose security modifications toward this end as a condition of granting approval to conduct the study. Only then is an IRB waiver of consent considered, and in fact, four conditions must be met: the research must be no more than minimal risk; the waiver must not otherwise affect the rights and welfare of the subjects; there is an impracticably requirement; and the subject must be provided with additional pertinent information.

There is an enormous problem, and I will summarize quickly. It has been my experience that most individuals are not aware that their medical records can legitimately be included in research without their express consent. This suggests that the IRB process, though well conceived, may fail to engender public trust if the communities so served do not fully understand the IRB authority to waive consent.

In legislation, consider such uses as uses of notices of information practices and a national educational effort to make clear the societal benefits of this class of research.

In conclusion, the current IRB function offers a strong model for protecting research uses of personal medical information. To be fully effective, however, a future IRB-like research review process would need to be widely expanded beyond the current IRB infrastructure. This expansion would need to be done in a way so as not to further burden the existence and the vital functioning of the existing IRB infrastructure.

Thank you.

[The prepared statement of Carolin M. Frey follows:]

PREPARED STATEMENT OF CAROLIN FREY, CHAIR, INSTITUTIONAL RESEARCH REVIEW BOARD, GEISINGER MEDICAL CENTER

Mr. Chairman and members of the Committee, I am Carolin Frey, PhD, Chair of the Institutional Research Review Board for the Geisinger Medical Center. I appreciate the opportunity to speak to you today specifically about the current role of the Institutional Review Board (or IRB) in protecting privacy as it relates to research.

Introduction and IRB as "model" for research review

The IRB I Chair reviews research originating from diverse parts of our multi-faceted health system which includes a distributed network of providers and a health maintenance organization. The health system relies on the free flow of medical information to ensure it travels with each patient at possibly distant geographic points of service. Our IRB, like others, has witnessed growth in research made possible by large pools of extant and identifiable medical information. We have taken a proactive role in setting standards for conducting this type of research. We do this, in part, because the IRB function has a lot to do with engendering public trust. To that end, the IRB function is a valuable model for independent review of research uses of personal medical information. With respect to pending privacy legislation, the IRB function is, however, only a model. It is not a ready-to-use resource. The current IRB system works well in the places it has been implemented but it does not provide universal oversight for research. There is also much latitude by institutions and IRB's in choosing how and when to review research based solely on extant and identifiable medical information. Legislation must distinguish between the existing IRB infrastructure and an "IRB-like" process that could be designed, albeit at substantial cost.

I will identify two limitations to the existing IRB function which would need to be overcome in legislating a process for universal review of research involving personal medical information.

IRB's currently oversee only a portion of human research

The existing IRB system was not designed to provide universal protections. Not all institutions conducting human research have an IRB and not all IRB's review

the special class of research involving extant and identifiable medical information. Institutions constitute IRB's usually because federally funded human research or investigations of FDA regulated products are done there. However, institutions may decide whether or not to apply the federal regulations to all research at that site or to just those studies required to meet the federal minimum. Many institutions extend the common rule to all research. However, when identifiable medical information travels between institutions it is possible for only portion of an individual's record to be within the purview of an IRB. For example, paper or electronic medical records in a hospital may be protected from privacy risks in research by virtue of the hospital IRB. However, when much of this same information travels to a third-party payor without an IRB it may no longer be protected should it become part of a research study. Complete, not partial, protection should be the goal of national legislation. To provide adequate protections, an "IRB-like" system would:

1) *have an orderly process for defining the purview of responsible reviewing entities to ensure complete and non-overlapping protections;* and
2) *be mandated at a sufficiently high federal level to ensure a review board is available at all locations where research on personal medical information takes place.*

The IRB role in protecting privacy is not well understood by the public

Where an IRB is used, its strength is in its authority to require strong security measures (sometimes likened to a "firewall") to protect the privacy of identifiable medical information used in research. However, the specific review procedures used, including exempting review altogether, the conditions necessary to waive consent and the societal benefits of research on personal medical information are not well understood. All of this amounts to inadequate understanding by the public of the risks (generally estimated to be small) and benefits (which can be quite great) of research on extant medical information.

The IRB function broadly provides protection of human subjects from physical, social, mental, privacy and confidentiality risks which might occur through participation in research. Much review is done during fully convened meetings attended by scientific and lay members both from within the institution and unaffiliated with it. Use of extant personal medical information is just one special class of research overseen by IRB's. An IRB may exempt from review, and hence any requirement for informed consent, some of this research if it involves "the collection or study of existing data, documents, records, if the information is recorded in such a manner that subjects cannot be identified, directly or through identifiers linked to the subjects." [46.101(b)(4)]. Again, some institutions have policies that go beyond the minimum regulation and require IRB review. For a variety of reasons, identifiers often must be retained. With recorded identifiers, such research generally qualifies for an "expedited" IRB review carried out by a single IRB member—usually the IRB Chair and sometimes a designate.

Expedited IRB review is a two step process. It is important to point out that "expedited" IRB review of research involving extant and identifiable medical information does not, by itself, result in an exception to the requirement to obtain the individual's consent for such use. First, consideration is given to whether the merit of the proposed research potential warrants an intrusion. The potential risk of that intrusion relies, to some extent, on the procedures proposed to ensure the security of the information. Security of research data protects against subsequent disclosures which are the primary risk of this type of research. In essence, a firewall can be built around research data and an IRB can impose security modifications towards this end as a condition of granting approval to conduct the study. There is some discretion concerning recommended security measures. Typically these include removal of personal identifiers from research records, use of coded study identifiers and separate safekeeping of a key which links the two. Restrictions to the sharing of research data with off-site investigators or potential future uses may also be made a condition of the IRB approval.

In a second step, the IRB may waive the requirement to obtain informed consent. This waiver is granted under the common rule only if the IRB finds and documents that "1) the research involves no more than minimal risk to the subjects; 2) the waiver... will not adversely affect the rights and welfare of the subjects; 3) the research could not practicably be carried out without the waiver...; and 4) whenever appropriate, the subjects will be provided with additional pertinent information after participation." [46.116(d)]

It has been my experience that most individuals are not aware that their medical records can legitimately be included in research without their expressed consent. This suggests that the IRB process, though well conceived, may fail to engender public trust if the communities so served do not fully understand this exception to gaining consent. The IRB review process, because it is not well understood, is not

likely to be seen as providing acceptable privacy protections. Legislation aimed at designing an "IRB-like" process should include additional provisions:

1) *use of notices of information practices* including a statement about disclosures for research purposes; and
2) *a national educational effort* to make clear the societal benefits of research involving personal medical information without consent.

Summary

Coordinated implementation of recommended privacy protections will be required to make these *transparent* to healthcare consumers. Without transparency, false consumer expectations may further erode public trust. Trust is key and trust will be hard to legislate. In addition to transparency, *uniformity* through preemption of state law to provide a "floor" (preserving greater protections by some state law) would help engender public trust. And finally, *accountability* in the form of audit trails for disclosures and the right to pursue actions against unauthorized uses of personal medical information are needed.

In conclusion, the current IRB function offers a strong model for protecting research uses of personal medical information. To be fully effective, however, a future "IRB-like" research review process would need to be widely expanded beyond the current IRB infrastructure. This expansion would need to be done in such a way as to not further burden the existing and vital IRB function. Institutional reviewing bodies would need to function with the complete support and cooperation of the institutions they represent. Most importantly, this would require, as part of communicating institutional information practices, complete disclosure of research activities to include a statement on how and when individual consent may be waived.

Thank you again for the opportunity to share information about the IRB function as it relates to privacy of identifiable medical information. I would be glad to answer any questions you may have.

Mr. BILIRAKIS. Thank you very much, Dr. Frey.

Before I yield to open the questioning by Mr. Greenwood, I would just like to remind you that the five of you are here because you are experts, because you have so much to offer to us, and this goes along obviously with the panel prior to yours. We don't have very much time to craft a piece of legislation. We are going to try to do everything we possibly can.

In fact, we have a meeting scheduled as early as 5 o'clock this afternoon to work with the minority to try to get something worked out. I am just inviting you to please keep that in mind. Any inputs you may have from a specific sort of standpoint in terms of legislation, don't hesitate. It will be very difficult for us to be able to contact every member of this panel and the other panel and get their inputs and crank them into what we are doing without your taking the initiative.

And the Chair at this point would yield to Mr. Greenwood.

Mr. GREENWOOD. Thank you, Mr. Chairman. Let me turn to Dr. Andrews.

Dr. Koski, respectfully, I differ with you in terms of your interpretation of the IRB aspects of the legislation, and Dr. Frey and others today have expressed differing views. I would like to give you an opportunity to comment on their comments or rebut anything that you think needs to be rebutted.

Ms. ANDREWS. Thanks very much.

I would first of all say I think the IRB mechanism is an invaluable one, and we depend on it heavily; and I would hate to overburden it because we need it desperately in cases of clinical research and any research that involves intervention or direct interaction with patients. And I think they do a marvelous job of safeguarding patient's well-being; and in many cases, they do look at data confidentiality issues.

My main concern is with the use of safeguards for observational research for which there is no medical risk to the patient and which relies purely on existing medical records. The existing structure—and I think one of the other speakers may have pointed out that a fairly small proportion of research that is currently being reviewed by IRBs is this type of information, so IRBs typically have less experience reviewing this kind of research. The typical procedure for reviewing this observational research using existing records is for it to be automatically assumed to be in the category of minimal risk, which then allows for an expedited review of only one member of the IRB.

And under the Greenwood bill, there are many more safeguards that we feel would provide greater safeguards for the handling of records and systematic review and procedures for the evaluation of research within the institution; and we feel that is much stronger, and having those safeguards in place would cover not only research where most researchers and others would agree there have been very few breaches of confidentiality, but would apply across the health care system in the cases where there have been breaches.

Mr. GREENWOOD. Thank you. Earlier, in the opening statements, some of the members on the other side of the aisle raised a legitimate point, and that is, why are we having this hearing just on my bill as opposed to other legislation?

I want to just give each of the panel members, in the time that I have left, an opportunity, if they choose, to either comment on, A, an aspect of—well, let us do it this way—to comment on any aspect or aspects of some of the other bills that have been introduced by members of this committee that you think either would be problematic and we would not want to incorporate, for a variety of reasons, into the final package; or where you think they are absent from the legislation under consideration today and ought to be incorporated. I won't put anybody on the spot, but if anyone would like to take that tack, it is an opportunity.

Ms. CARTY. I will speak specifically to the issue that I raised in my earlier testimony, which is the preemption of State law, and I think that is a major issue because I know your bill, Congressman Greenwood, very responsibly establishes that ceiling that would allow the really critical research to continue uninterrupted throughout the 50 States. By establishing a floor, as reflected in H.R. 1941, we would see a multitude of States enacting legislation really making some critical research areas completely unworkable, and it would certainly, the degree—I am sorry.

Mr. GREENWOOD. If I could interrupt you, because that point has been disputed by, particularly, other members of the first panel. Could you try to illustrate that in some way with something specific?

Ms. CARTY. Sure, a specific example—and actually I will move outside of the State of California, because we are in sort of a strange period right now where the State legislature is reviewing at least 4 or 5 bills that will probably make it through the legislature. But I know that the committee has already received testimony from Dr. Steven Jacobson from the Mayo Clinic, and I think the point that he brought in terms of Minnesota enacting specific requirements, consent requirements, and the effect that those re-

quirements actually had on the data that the researchers eventually had compiled, was quite troubling. For example, women were more reluctant to go the extra mile in terms of giving that actual consent. People who are younger were more reluctant to give that consent. People with history of mental health issues were more reluctant to give that consent.

So would that skew the research? Absolutely. And compound that times whatever, how many other States would enact that type of legislation? Would it skew the research? Absolutely, and certainly the research would be carried out in a much slower fashion; and there are certainly some research areas that would just not be explored because it would be unworkable.

Mr. GREENWOOD. At the chairman's discretion, are there any other members of the panel that want to respond?

Mr. BILIRAKIS. Any very quick responses or short responses?

Mr. KOSKI. I will try to be very quick.

I think that 2470, as it now stands, is the right start, but it is deficient in a number of perspectives. One is, it could allow release of information to third parties that is identifiable information for which it may not have been originally intended. I think those provisions need be tightened up quite extensively.

Also, the provision of penalties for inappropriate uses of information I think needs to be strengthened as well. There should be a requirement for active information, delivered to patients regarding policies for how their information is going to be used and protected at every entity where it is going to be collected; the bill is deficient there. In terms of—well, I won't—I already covered the issue of using different classes of information.

But in this particular—this bill's description of nonidentifiable is totally inadequate. Coded information that can be directly linked back to an individual is identifiable. It may be coded deidentified, but it is nonetheless identifiable, and if you are going to ask someone to give up their rights to determine what is done with information, tissues and all that can be linked back to them, you have got a problem. They have to authorize that.

I think we need to be very explicit. Nonidentifiable and identifiable are mutually exclusive. You can either tell who it came from or you can't. So I think we need to avoid that term, change that definition so that we make what is nonidentifiable. That would serve a great deal of research purposes and have essentially no risk associated with it whatsoever and would be very helpful.

Mr. BILIRAKIS. The gentleman's time has long expired, but of course, that is the sort of thing we would like to get from you in writing to help us out here.

Mr. KOSKI. It is in my written testimony.

Mr. BILIRAKIS. I am not sure it is in response to the question. I think he was looking for something to the opposite.

Mr. Brown.

Mr. BROWN. Thank you, Mr. Chairman.

Mr. Johnson, you argue in your testimony that uncertainties in the laws should be clarified not through private right of action but, quote, "through administrative regulations that will flesh out the many rights, responsibilities and protections in the legislation," an interesting approach from the Chamber of Commerce, asking for

more government regulations, I might point out. But along these lines, compare if you would, administrative authority, if this is what you are really asking for, some fleshing out through rules and regulations. The administrative authority in the Greenwood bill, what the administrative authority—language found throughout the Condit bill, which is preferable, to get us to the point where we really know more about private course of action and whether we, in fact, really need that private right of action?

Mr. JOHNSON. Well, Congressman, I have to admit I am not familiar with the Condit bill. I haven't looked at how they flesh out the administrative obligations there. My reference to the obligation of HHS to flesh out responsibility was simply based on the fact that the Greenwood bill has the kind of general authority provision given to HHS to issue regulations. But it is not inconsistent with the typical position of the Chamber of Commerce, I don't think; and here we are looking at—we are not necessarily happy about a new law that is going to impose new mandates on our members. We are trying to get to a point where it is the least objectionable possible.

There is no question about the fact that between an administrative regulation that tries to set some guidance—and we hope the rulemaking is a good one—and a private cause of action across the Federal courts, my members would prefer the former. So we are trying to pick sort of what is the line of least resistance, I believe, here. And I am not saying we are happy with either one, Congressman, and I do apologize about the Condit bill. I am not just not familiar with that.

Mr. BROWN. I think that sort of illustrates how important it is—I know the chairman actually agrees on this—in the future, when we are considering legislation like this, we need to look at all the pieces of legislation that have been offered. The numerous Federal privacy laws relating to other types of information include a private right of action: The Fair Credit Reporting Act, which sets forth confidentiality protections on a consumer's credit report; the Video Privacy Protection Act, which sets forth confidentiality protections on consumer's video rental records; the Cable Communications Policy Act, which sets forth privacy protections related to information about cable service subscribers.

How can we have laws protecting allowing an individual right of action on cable subscribers, video rental records, Mr. Johnson, and not do that with something as important as medical privacy, the most important, intimately important, information almost and maybe, perhaps, the most intimate information attached to an individual?

Mr. JOHNSON. Well, Congressman, I would ask that when those comparisons are made that your staff and you take a real close look at those statutes and ask—they may have a private cause of action, do they have the same kind of very severe criminal and civil sanctions that the Greenwood bill does? My guess is no. They have one or the other, or some very moderate types of penalties and a private cause of action. I would also ask that you look at what is the obligation that is being addressed in those laws.

You mentioned the video rental law. Let me read the definition of what is the protected information there. The term "personally identifiable information" includes information which identifies a

person as having requested or obtained specific video materials or services from a videotape service provider. The defendant in that kind of case knows what their obligation is. The law is very narrow, what they are trying to regulate, which is disclosure of, did you rent or buy a videotape? The law is very understandable in that case.

I think if you compare that definition to what is in the Greenwood bill or any of these bills that go to health confidentiality, you will see that one is a very small, understandable legal obligation as compared to a very amorphous obligation. Therefore, the more amorphous an obligation is, the more difficult it is to understand, the more exposure there is to an employer or a business in court and a vague reason, jury trials. So you have to look at the whole combination of the law is what I am saying.

And third I guess I would just say that every law is different. Every law goes through its own negotiations as it goes through the congressional process. Sometimes some provisions get more attention than others. I have seen that. I have spent 9 years on the Hill. Sometimes provisions such as enforcement didn't get the close scrub they should have. So parallels sometimes I think just have to be looked at carefully.

Last, I would say there are many important rights as identified in my testimony, such as safety and health in the workplace, that don't have private causes of action; and I don't think any of us will argue that OSHA is a slouch in enforcement or the National Labor Relations Board is a slouch in enforcement, and yet these are very important rights that Congress has chosen not to protect through a private cause of action.

Mr. BROWN. Some might argue that OSHA doesn't have the authority it needs in protecting workers. Not too many of our members would argue that I am sure.

Mr. BILIRAKIS. I thank the gentleman. I am going to hitchhike on Mr. Brown's questions.

Mr. Johnson, are there remedies in tort law today that would be available in the event an individual wanted to bring a cause of action as a result of breach of confidentiality?

Mr. JOHNSON. Well, it is my view, and I think it is the view of other people who have looked at this bill, that the Greenwood bill does not preempt tort laws such as intentional infliction of mental distress, which would apply therefore to your worse kinds of situations.

Mr. BILIRAKIS. So there are remedies in tort law existing today?

Mr. JOHNSON. It is not going to cover every single legal obligation.

Mr. BILIRAKIS. No law does.

Mr. JOHNSON. No law does.

Mr. BILIRAKIS. Are you aware of any cases where an individual had the confidentiality of their medical records compromised and yet they were unable to bring a court action?

Mr. JOHNSON. I personally have not.

Mr. BILIRAKIS. Are any of you aware of any similar case where they just weren't able to bring a court action because a remedy was not available?

Ms. Carty, you touched on this and, in a sense, I suppose maybe you answered it. Currently 34 States, as I understand it, have laws governing access to medical records. A major clinical trial would be administered in possibly dozens of States, one trial in possibly dozens of States. Won't the complexity and cost of research be driven up? It may even be impossible to be adequately conducted, if you will, if researchers instead of meeting a single uniform standard must tailor their programs in multiple ways in order to gain access to data in a number of States?

Ms. CARTY. Yes, Mr. Chairman. I think it is important to recognize that when a biomedical company decides to pursue a line of medical research, there are many factors that are involved—cost, of course. If that were the case and that continues to move on in terms of the State legislation and a multitude of State laws, would it increase costs? Absolutely.

Would it also result in some treatment simply—some lines of science and some treatments not being explored? Yes, absolutely, it would certainly have a major impact.

Mr. BILIRAKIS. You were in the audience when Dr. Appelbaum testified and used the illustration of people come from Vermont, New Hampshire travel into Massachusetts and therefore it is Massachusetts law which applies, but if the research touched upon people in every one of those locales, you will have actually different laws that would apply. It wouldn't be just Massachusetts law; it would be Massachusetts, Vermont, New Hampshire, Rhode Island, et cetera, right?

Ms. CARTY. That is correct.

Mr. KOSKI. May I respond to that, Mr. Chairman?

Mr. BILIRAKIS. If you do it quickly. We have a vote on the floor, unfortunately. I apologize, but that is the way things are up here.

Mr. KOSKI. I think that Ms. Carty's response there is really somewhat self-serving.

Mr. BILIRAKIS. Self-serving?

Mr. KOSKI. Yes, self-serving in terms of the industry.

Mr. BILIRAKIS. You guys are tougher on each other than we are.

Mr. KOSKI. I think, in fact, for a clinical trial, the example that you cited, in every one of those cases, a patient is going to be giving written informed consent. Currently, institutions all have their own requirements for access to medical records. The situation that would be imposed by individual legislation in different States is probably not going to be any more cumbersome with respect to doing multicenter clinical trials than the current situation. Having said that, though, I would say that the concerns about preemption to a large extent, I think, are separated with where one sets the floor. If you have a national standard that was set as a platform rather than a floor, and people were comfortable with that, I suspect that, you know, a few States would feel obligated to go beyond those provisions, and the concerns about preemption would not——

Mr. BILIRAKIS. Not very many, in other words, would be obligated. A response, Ms. Carty?

Ms. CARTY. Mr. Chairman—and I know you have to get to your vote, but I just want to respond by bringing up the issue of genetic research.

If States crack down on the use of genetic information, forbid the use of genetic information in research studies, there are whole lines of research that will not be explored; and not really considering this self-serving, I mean, really talking about, I think, the patients, the Alzheimer's patients and the breast cancer patients would probably be happy with that kind of self-serving statement because it is those lines of research we can hope to explore through a responsible flow of genetic information.

Mr. BILIRAKIS. The clock wasn't turned on, but I think probably my time is up.

Mr. WAXMAN. I want 5 minutes but I don't think I have 5 minutes now. May we vote and then return?

Mr. BILIRAKIS. I guess we are going to have to do that.

Mr. HALL. I can take my 1 minute now if you would like me to.

Mr. BILIRAKIS. All right. The gentleman is recognized.

Mr. HALL. Just to respond to Mr. Johnson that I agree with his ideas about OSHA, and I think they have way too much authority and don't use it very wisely.

I yield back my time. That is all of it.

Mr. BILIRAKIS. Well, all right. Mr. Burr was on his way back, but I understand there are two votes, so he probably is held up. So we are going to have to recess for just a few minutes until we can get back. I am sorry. Thank you.

[Brief recess.]

Mr. BILIRAKIS. The hearing will come to order.

Where were we? Mr. Waxman.

Mr. WAXMAN. Thank you, Mr. Chairman.

Dr. Andrews, I understand that you were the Chair of the International Society for Pharmacoepidemiology when it issued its 1997 recommendations on medical record confidentiality, and that report stated that all pharmacoepidemiologic studies that use personally identifiable data should be subject to IRB approval before a study commences. It noted that the IRB mechanism has been and should continue to be the keystone for protecting patient confidentiality by evaluating the use of potentially identifiable data, considering such use in the light of privacy and confidentiality, and further legislation should protect and strengthen IRB's ability to waive individual informed consent under these circumstances.

This seems different than the views you expressed today.

Mr. ANDREWS. Let me expand on that. Our committee continues to look at this in a great deal of detail. We were addressing mainly the issue of studies that require review of very identifiable records in medical institutions to identify patients to whom—who would be approached to consent to participate, for example, in a case control study of birth defects. We wanted to make it very clear that there is a role for IRBs to review this kind of research which would fall under the category that I mentioned earlier of interventional research in which a patient will ultimately be contacted.

Mr. WAXMAN. It says to balance the individual privacy interest with society's need for sound information based on medical and public health issues, we should build on current laws and ethical guidelines, including the use of institutional review, ethics committees or their equivalent, that have served well in the past.

Among their specific recommendations were the following: All pharmacoepidemiologic studies which use personal, identifiable data should be subject to IRB approval before study commences. The IRB mechanism has been and should continue to be the keystone for protecting patient confidentiality by evaluating the use of potentially identifiable data and considering such use in the light of privacy and confidentiality.

Mr. ANDREWS. Absolutely, and let me clarify it. I think that everything revolves around the definition of what is considered identifiable or nonidentifiable. The way most epidemiologists and researchers would define nonidentifiable data would be information which is maintained in a form in which direct patient identifiers have been stripped and replaced with a code which could potentially be linked back but which are not, on the face of it, identifiable to the researcher. And that information—the kinds of studies that we use that kind of key coded information would be considered in our profession to be nonidentifiable data.

Mr. WAXMAN. Isn't that a common rule and wouldn't—let me put it this way, because I don't want to argue with you. It seems hard for me to reconcile your testimony here with the statements which take such strong positions for IRBs when the patients are going to be identified. Maybe you can elaborate, and I would want the chairman to hold the record open if you want.

Let me continue on because I only have 5 minutes. Dr. Koski, you believe IRB oversight should be extended to all health researchers. Could you elaborate on this view and comment on the guidelines for health researchers' review that are in the Condit-Waxman bill and the Greenwood bill?

Mr. KOSKI. I don't think that there is a need to extend it so much with respect to the common rule, but rather to make sure that the common rule is extended to all of the IRBs.

Mr. WAXMAN. That is what I meant. You would have it apply not just to government funded studies, but all private studies?

Mr. KOSKI. Exactly. I would support that strongly. I think that would provide the most robust system for protection of human subjects in research, and I think there needs to be appropriate resourcing to get that done.

I do think that 1941 has a useful section in its research sections that provides some beginning guidance for developing specific policies, guidelines for the use of identifiable health information, and those might be valuable to consider as we work toward a final type of legislation that would emerge in this process.

Mr. WAXMAN. You would want to see IRBs and not something equivalent to IRBs?

Mr. KOSKI. Absolutely, Mr. Waxman. I believe that having a separate process that causes a segregation in the whole process for review and approval of research would not only undermine the process that is there, it would tend to dilute the process for protection of human subjects and I think that would be a serious error.

Mr. WAXMAN. You don't think that will hinder research?

Mr. KOSKI. No, it will make it better because by protecting human subjects and by letting them know that we are putting their interests in the appropriate priority, there will be a greater willingness to participate in research, and I think I would like to make

very clear to my colleagues here that in no way are the IRBs opposed to research. Our institutions live on research. That is what we do. Our goal is to make sure that research is not only done, and the best research is done, but that it is done right.

Mr. WAXMAN. I think I heard the bell, Mr. Chairman.

Mr. BILIRAKIS. Yes, some time ago.

Mr. WAXMAN. Well, I yield back the balance of my time.

Mr. BILIRAKIS. Mr. Burr, to inquire.

Mr. BURR. Thank you, Mr. Chairman. Ms. Carty, it has been quite awhile since you testified. I want to take the opportunity to restate something that I heard you say. You said there are significant health benefits to national uniformity providing access to medical records. Did I understand you correctly?

Ms. CARTY. That is correct.

Mr. BURR. There are significant health benefits to uniformity?

Ms. CARTY. Yes, within a scope of potential therapies that can be researched and developed through responsible areas of clinical testing research.

Mr. BURR. Again, like I did with the last panel, I want to try to bring this whole question back to the quality-of-health focus on the patient. I understand, Mr. Koski, you have got a very specific area that you have proposed, not even flexing over to a modified IRB, and I want to make sure that we all concentrate on the patient for a minute when we are talking about—is the IRB the best way, when we discard some potential research that might be done, let us understand who is affected. It is a patient. It is somebody we don't know. It is somebody that potentially is sick, somebody potentially that is terminal. And the question is: Are we going to do everything we can to encourage the development? Let me ask you, if you had 50 different State rules, what would that do to the development of technology in medicine?

Ms. CARTY. It would slow it in some areas. It would stop it in some areas. And that is the range. And that means very practical implications for the patients and their families. Let me give you a very practical example.

The magazine Nature came out with a wonderful article describing some areas of research in Alzheimer's disease, the potential development of a vaccine. This research is moving from conduct in mice in the labs and is just about to move into human clinical trials.

I would absolutely submit today that if uniform standards are not adopted, that that will directly impact the quality of that research, those clinical trials and that observational research that will be conducted over the next phase in developing this vaccine.

Mr. BURR. Let me ask, because Mr. Koski talked about—you suggested that the definition of nonidentifiable information in the Greenwood bill is too broad and that any ability to link back information should render it then by definition identifiable.

I remember meeting with a company that does research and they told me about one specific study of a drug that was out, and the specific instructions from the manufacturer to the physician was no more than one prescription because of a potential risk with multiple prescriptions of liver problems. And the company was so concerned that doctors didn't read their directions that they had this

company in an identifiable way go and research. And they found that doctors were prescribing multiple prescriptions, at which time the company pulled the product off the shelf because of potential liver damage.

Let me ask you to talk about the nonidentifiable and identifiable situation that we run into and what significant problem that will create when we talk about public health.

Mr. ANDREWS. Well, I am very concerned about the possible implications for public health, because in the area specifically of drug safety monitoring, we rely on large data bases of existing records that cross State lines and come from health maintenance organizations and other places. We simply must be able to have access to that kind of information to rapidly address important public health questions. If that information is key-coded but the researcher has no way of identifying the individual patient, the researcher does not want to know who the individual patients are, but it is important to maintain the link back to the original medical record.

Mr. BURR. Let me ask, the company that I met with, they maintain the key. Now, it is up to them to maintain the privacy of the key to protect its integrity. What is wrong with them maintaining the key if, in fact, somebody had to for health reasons trace back to a particular person for public health reasons? Is there any problem with that?

Mr. ANDREWS. Who would be maintaining the key?

Mr. BURR. Whoever we put in charge. In this particular case it was the company that I met with, they control the key to the identifier. Things go out unidentified. What you said, even if it went out nonidentified, the fact that there was a key and the company had the key, you could not trust the integrity of their maintaining the privacy of the key, therefore it should be identifiable; is that correct, Mr. Koski?

Mr. KOSKI. More or less.

Mr. BURR. Without some ID capabilities, how could you ever trace back a public health problem?

Mr. ANDREWS. You probably couldn't. It is important to be able to validly evaluate public health problems. If you have strictly nonidentifiable data and look through very large data sets, you may find a medication that is associated with several cases of very serious medical problems, life threatening fatal problems. You would hate to take a drug off the market because of those problems, if you assumed the drug caused it, without going back through the appropriate channels and finding out more information about those specific cases to find out if there were other explanations, which inevitably there might be.

And that is one of the reasons that it is important to maintain the key for—to validate the study, to collect additional data, to supplement the study that has been done using identifiable data, and those are the circumstances in which a study would normally go to an IRB or some mechanism that is created to evaluate under what circumstances is it appropriate to go back to contact the patient.

Mr. BURR. If you open this process up to an IRB or modified IRB, let me ask you, an extended liability to the degree that some have suggested, what would be the willingness of participants to participate as part of the IRB, knowing that if there was a breach of the

responsibility of confidentiality of the IRB that they were personally liable?

Ms. FREY. I can't speak for all IRBs but in ours we are a function of the institution so our IRB members are covered with liability insurance on the part of the institution.

Mr. BURR. What would the institution's position be?

Ms. FREY. That brings up who the owner of the data is. IRBs serve a vital function but they are not data custodians and they are not owners and they are still charged by the institutions that host the data.

Mr. BURR. But the individuals who make up the IRB would be the people who determine whether it is appropriate to move forward?

Mr. WAXMAN. Will the gentleman yield?

Mr. BURR. I don't have any time, but I will be happy to yield.

Mr. WAXMAN. All of these questions about the dangers of having an IRB go through and look at identifiable information about a patient, this is what is done now, and so much of the research——

Mr. BURR. I didn't raise a question about IRBs going in as currently written. My question to Dr. Koski and Dr. Frey was if we increased—which some have suggested even today the exposure to liability by individuals who make decisions about whether privacy should be maintained—if that privacy were breached and individuals who make up the IRBs were liable individually or as a group, my question is: Would that affect the willingness of people to participate in IRBs?

Ms. FREY. The obvious answer is yes. I would not propose, however, that that be the chain of liability. In fact, the very title of an institutional review board is just that. It is an institutional function. And in fact, there are cases where institutional review boards are found deficient because of institutional problems, not because of any deficiencies or lack of knowledge on the part of the members.

I think it is important to keep in mind and distinguish data ownership and charge of responsibility with the people who actually carry out the charge. The reality is that in carrying out that charge, there is a very extensive process of documentation, the Federal code is very clear, and I don't think that any audit would point easily to an individual having made a mistake. It would be difficult, I will not say inconceivable.

Mr. BILIRAKIS. The gentleman's time has expired.

Mr. WAXMAN. I wanted to jump in on this, but I don't know how you want to proceed.

Mr. ANDREWS. I would like to make a comment about IRB participation if that is okay.

Mr. BILIRAKIS. Make your comment.

Mr. ANDREWS. I think it is vital that we have people willing to serve on IRBs. IRBs serve an incredibly important function in this country. I think people would be more willing to serve on IRBs if there were adequate protections on the movement and processing of information within the institution. I think in the Greenwood bill there are internal processes and safeguards that are set up, which IRBs tend to rely on, and those safeguards are stronger than what exists now and those are Federal—they would be uniform and fed-

erally enforceable, and I think that would provide a level of safeguards higher than what we have now.

Mr. WAXMAN. But that is only an accurate statement as to research that is not now touched by the common rule, because if it is research touched by the common rule, which means there is Federal nexus to that research, then there is a stricter requirement that if there is use of information that is identifiable to a particular patient, then either they have to get consent or go to an IRB to get the IRB to agree that consent is not going to be necessary for this public purpose.

Since it is being done in so much research now, I have not heard why that is a problem if we applied it to research being done that is strictly private. The Greenwood bill has a provision for something akin to an IRB for that private research. You can say that it is better than what we have now because now there is nothing there; but it has deficiencies, as many of us see it, particularly since that internal review process could involve a conflict of interest with those people who are sitting on that IRB. Am I misreading that?

Mr. BILIRAKIS. We don't want to go on indefinitely here. Maybe a pro-and-con response and then we will finish up.

Mr. ANDREWS. Two quick points. You are correct, the studies are covered by the IRB regs, but what typically happens because data studies based on existing data are considered to have minimal risk, they are reviewed through the expedited review mechanism, which means that one member, generally an employee of the institution, does that review.

The other comment is that most IRBs typically, according to the GAO report, rely on the policies that are in existence in the institution for the handling of archival medical records.

Mr. WAXMAN. In other words, it has worked reasonably well?

Mr. ANDREWS. We are suggesting——

Mr. WAXMAN. Because they have these expedited procedures, why would you object to having this same procedure used for private research?

Mr. ANDREWS. We are suggesting that it is not working terribly well. Not much of the observational research is going to IRBs. We feel that we can have greater safeguards which would encourage more research to be done if we had the safeguards with federally enforceable national standards that would be in place.

Mr. KOSKI. I think, in fact, the answer is to be sure that research that is not currently going to IRBs does go to IRBs under a reasonable set of guidelines for review of this kind of information. In fact our own policies for confidentiality and privacy are far stricter than what is in the Greenwood bill. So if we subscribe to that, it would definitely undermine the protections we already have in place. It would be a mistake.

Ms. FREY. I heard conflict of interest. Yes, an expedited review may be carried out by one member. Institutions generally have written policy concerning conflict of interest and in that case the review would necessarily go to someone without a conflict of interest.

Mr. WAXMAN. Do you read the Greenwood bill as permitting a possible conflict of interest?

Ms. FREY. I am not familiar with the exact language of the bill.

Mr. BURR. I ask that the staff on both sides, majority and minority, as well as Mr. Greenwood, if they are meeting with Dr. Feldblum tonight, since she is a lawyer from a reputable school and also familiar with this situation, just ask about the liability issue; because one of the further concerns would be could, if the institution were liable, could it then influence the decision of the members of the IRB because of pressure from the institution?

Mr. WAXMAN. An issue that I have not heard raised except by you today.

Mr. BURR. I have been accused of raising things never raised before.

Mr. GREENWOOD. Always on the cutting edge.

I thank the chairman and the panel who stayed for 6 hours for this hearing, and to reiterate the commitment that I made in my opening remarks that this is important and we all share the same interest.

Mr. BILIRAKIS. It is important and we can work together outside of politics.

There are always written questions that the committee has of the panelists, and we would appreciate, obviously, quick responses to them because we don't have that much time. Thank you very much. It has been a good hearing and you have helped to make it so. The hearing is adjourned.

[Whereupon, at 4 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

PREPARED STATEMENT OF HON. CHRISTOPHER SHAYS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CONNECTICUT

Chairman Bilirakis, Ranking Member Brown and members of the Subcommittee:

Thank for the opportunity to provide you with my thoughts on medical records confidentiality as you consider H.R. 2470, the Bipartisan Medical Information Protection and Research Enhancement (MIPRE) Act, which was introduced by Representative Jim Greenwood to protect the security of patients' medical information.

As an original cosponsor of H.R. 2470 and a sponsor of H.R. 2455, the Consumer Health and Research Technology (CHART) Protection Act, I firmly believe this Congress must enact comprehensive medical records privacy legislation.

There is currently no comprehensive, uniform standard to protect the privacy of a patient's medical records and there have been several startling examples of the potential effects of this void over the past several years. For example, USA Today reported in 1996 that a public health worker in Tampa, Florida walked away with a computer disk containing the names of 4,000 people who tested positive for HIV. The disks were sent to two newspapers.

In addition, The National Law Journal reported in 1994 that a banker who also served on his county's health board cross referenced customer accounts with patient information and subsequently called due the mortgages of anyone suffering from cancer.

Under the Health Insurance Portability and Accountability Act (HIPAA), should Congress fail to enact comprehensive legislation to protect the confidentiality of medical records by August 21 of this year, the Secretary of Health and Human Services will be required to promulgate regulations.

I believe our colleagues on both sides of the aisle have come to recognize the need for Congress to act before the Secretary steps in. I was encouraged by the inclusion of medical records confidentiality provisions in the Financial Services Act which the House recently passed. The provisions were an important first step toward recognizing the need for legislation to ensure the confidentiality of medical records but alone they are not sufficiently comprehensive to guarantee the privacy of individual patient records.

In my opinion, the question is no longer "*Will* Congress act before the August deadline?" but "*How* will Congress act before the August deadline?"

While this hearing is focused on the consideration of the MIPRE Act, I wanted to take the opportunity to bring to the Committee's attention the CHART Protection Act, which I recently reintroduced, and highlight several important similarities and differences between the two pieces of legislation.

The CHART Protection Act shares a number of important provisions with the MIPRE Act. Both bills allow patients to inspect, copy and where appropriate, amend their medical records.

In addition, both bills impose strong criminal and civil penalties to deter abuse and increase incentives to use non-identifiable information.

Finally, both CHART and MIPRE allow for the use of protected information for research purposes when reviewed by an Institutional Review Board or where the individual has provided specific authorization.

Focusing on the differences between the two bills, I would like to briefly outline the unique approach the CHART Protection Act takes to ensure the confidentiality of medical records, and touch on how the legislation differs from the MIPRE Act in two crucial areas—authorization for use of individually identifiable health information and preemption of state law.

The MIPRE Act and other bills restrict the use of health information unless it is specifically authorized for disclosure. Rather than spelling out the individually identifiable information which can be disclosed, the CHART Protection Act sets forth the inappropriate uses of protected information and allows for disclosure of individually identifiable information unless it is specifically prohibited in the bill.

Use of anonymous information will not be affected by the CHART Protection Act unless the information is intentionally decoded and used to identify an individual.

The MIPRE Act creates a statutory authorization which permits the disclosure of protected information if it is permitted in statute. The bill sets out permissible uses of individually identifiable information and prohibits all other uses unless they are specifically authorized by an individual.

In my opinion, a shortcoming of this approach is that it permits the disclosure of health information for a variety of activities without patient consent. In fact, there is nothing in the act requiring an authorization from the patient to use information if it falls within the statutory authorization.

The approach taken in the CHART Protection Act gives patients more control over their medical records by requiring authorization for a majority of uses of individually identifiable information.

The CHART Protection Act creates a consolidated authorization process for the use of individually identifiable information by providing the authorization up front, but allows individuals to revoke their permission for health research purposes at any time.

The CHART Protection Act generally preempts state law except mental health and communicable disease protections enacted by states and localities, as well as public health laws such as birth and death reporting.

In contrast, the MIPRE Act preempts state mental health and communicable disease laws, and may serve to weaken state laws which are more stringent than federal statute.

Mr. Chairman, despite their differences, and despite my belief that the overall approach taken in the CHART Protection Act offers more stringent protections to consumers, the MIPRE Act represents a comprehensive approach to protecting the confidentiality of medical records while protecting legitimate uses of medical information.

It is my hope that my colleagues will work toward passing a uniform and comprehensive confidentiality law which serves to balance the interests of patients, health care providers, data processors, law enforcement agencies and researchers.

Thank you for the opportunity to submit my testimony.

CMS Library
C2-07-13
7500 Security Blvd.
Baltimore, Maryland 21244

CMS LIBRARY
3 8095 00006798 9

ISBN 0-16-059576-2
90000
9 780160 595769